НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Інформаційно-телекомунікаційних мереж

До захисту допущено:

Завідувач кафедри

_____ Лариса ГЛОБА

«___»_____2020 р.

Дипломна робота

на здобуття ступеня бакалавра
за освітньо-професійною програмою «Інформаційно-комунікаційні технології»
спеціальності 172 «Телекомунікації та радіотехніка»
на тему: «Аналіз методів захисту інформації в мережі IP-телефонії»

Виконала:
студентка IV курсу, групи ТІ- 61
Корман Наталія Анатоліївна _____

Керівник:
Професор кафедри ІТС ІТС, професор, д.т.н.,
Могилевич Дмитро Ісакович _____

Рецензент:
Доцент кафедри ТК ІТС, доцент, к.т.н.
Явіся Валерій Сергійович _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

Студентка _____

Київ – 2020 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
Кафедра Інформаційно-телекомунікаційних мереж

Рівень вищої освіти – перший (бакалаврський)
Спеціальність – 172 «Телекомунікації та радіотехніка»
Освітньо-професійна програма «Інформаційно-комунікаційні технології»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Лариса ГЛОБА
«___»_____2020 р.

ЗАВДАННЯ

на дипломну роботу студенту

Корман Наталії Анатоліївні

1. Тема роботи «Аналіз методів захисту інформації в мережі IP-телефонії», керівник роботи професор кафедри ІТМ, д.т.н., професор Могилевич Дмитро Ісакович, затверджені наказом по університету від «30» березня 2020 р. № 924-с

2. Термін подання студентом роботи 8 червня 2020 р.

1.Спеціальна література, матеріали мережі інтернет

2.Наукові статті про підвищення рівня інформаційної безпеки

3.Використання криптографічних методів шифрування для захисту даних

4. Зміст роботи:

1. Аналіз основних причини несанкціонованого доступу до інформації в мережі IP-телефонії, їх класифікація та призначення.

2. Порівняльний аналіз ефективності застосування протоколів шифрування, виділити переваги і недоліки методів криптографічного захисту інформації на основі VPN.

3. На основі практичного аналізу криптографічних протоколів захисту інформації показати найбільш продуктивний метод збереження цілісності даних.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо):

Слайд №1 – Тема роботи;

Слайд №2 – Актуальність роботи;

Слайд №3 – Мета роботи;

Слайд №4 – Практична цінність роботи;

Слайд №5 – Задачі, які виконуються в роботі;

Слайд №6 – Висновки по роботі;

6. Дата видачі завдання 10 вересня 2020 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Підготовка і вивчення літератури	до 25.09.2020	Виконано
2	Розробка вступу	До 27.02.2020	Виконано
3	Розробка 1 розділу	До 18.03.2020	Виконано
4	Розробка 2 розділу	До 12.04.2020	Виконано
5	Розробка 3 розділу	До 22.05.2020	Виконано
6	Оформлення роботи	До 08.06.2020	Виконано

Студент Наталія КОРМАН

Керівник Дмитро МОГИЛЕВИЧ

РЕФЕРАТ

Робота містить 65 сторінки, 28 рисунків та 10 таблиць. Було використано 26 джерел.

Метою роботи є підвищення захисту мовної інформації в мережі IP-телефонії на основі аналізу методів захисту інформації від несанкціонованого доступу, що можуть бути реалізовані навмисним впливом природного або штучного характеру.

В даній роботі розглядаються основні аспекти побудови віртуальних приватних захищених мереж, їх класифікація та призначення, принципи їх побудови, необхідні умови для повноцінного функціонування. Досліджено основні методи захисту інформації від несанкціонованого доступу, що можуть бути реалізовані впливом природного або штучного характеру у VPN мережах.

Наведено характеристики всіх основних видів загроз на інформацію. Проаналізовано основні криптографічні методи захисту інформації на основі VPN-мережі. Наведено переваги та недоліки, які притаманні протоколам шифрування.

Досліджено вплив шифрування на канал зв’язку OpenVPN, проаналізовано пропускну здатність та ефективність використання складних криптографічних методів. Для досягнення поставленої мети було проведено практичне виконання залежності пропускної здатності OpenVPN від параметрів шифрування, було описано та проведено налаштування OpenVPN серверу на базі операційної системи Ubuntu, а також процес створення конфігурації для клієнта.

Отримані результати дозволяють ефективно обирати відповідно до типу інформації та способу її передачі шифри, що максимально задовільнять високий рівень захисту, та більшу продуктивність.

Ключові слова: VPNмережа, технології побудови віртуальних мереж, протоколи шифрування.

ABSTRACT

The work contains 65 pages, 28 figures and 10 tables. 15 sources have been used.

Goal: is an analysis of the main methods of protecting information from unauthorized access, which can be implemented under the influence of natural or artificial nature.

This paper considers the main aspects of building virtual private secure networks, their classification and purpose, the principles of their construction, the necessary conditions for full operation. The main methods of protecting information from unauthorized access, which can be implemented by natural or artificial influences in VPN networks, have been studied.

The characteristics of all major types of information threats are given. The main cryptographic methods of information protection based on VPN-network are analyzed. The advantages and disadvantages of encryption protocols are presented.

The influence of encryption on the OpenVPN communication channel is studied, the bandwidth and efficiency of using complex cryptographic methods are analyzed. To achieve this goal, the dependence of OpenVPN bandwidth on encryption parameters was practically implemented, the OpenVPN server based on the Ubuntu operating system was described and configured, as well as the process of creating a configuration for the client.

The obtained results allow to effectively choose ciphers according to the type of information and the way of its transmission, which will satisfy the highest level of protection and higher productivity.

Key words: VPN network, virtual network building technologies, encryption protocols.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АРМ	автоматизоване робоче місце
АС	автоматизована система
МЕ	міжмережевий екран
НСД	несанкціонований доступ
ПЗ	програмне забезпечення
ПК	персональний комп’ютер
3DES	(Triple Data Encryption Standard) – симетричний блочний шифр
ACL	(Access list) – список управління доступом
AES	(Access list) – список управління доступом
AH	AES (Advanced Encryption Standard) – симетричний алгоритм блочного шифрування
CLI	(Command-line interface) – різновид текстового інтерфейсу
DES	(Data Encryption Standard) – симетричний алгоритм шифрування
DH	(Diffie–Hellman) – криптографічний протокол
ESP	(Encapsulating Security Payload) – протокол забезпечення безпеки трафіку
HMAC	(Hash-based message authentication code) – механізм перевірки цілісності даних
HTTP	(Hyper Text Transfer Protocol) – протокол передачі даних
IANA	(Internet Assigned Numbers Authority) – функція керування просторами IPSec
ICMP	(Internet Control Message Protocol) – мережевий протокол
IETF	(Internet Engineering Task Force) – міжнародне співтовариство
ICV	(Ntegrity Check Value) – алгоритм перевірки даних
IKE	(Internet Key Exchange) – протокол набору протоколів IPSec
IOS	(Internetwork Operating System) – міжмережева операційна система
IP	(Internet Protocol) – протокол міжмережевого рівня
IPSec	(IP Security) – набір протоколів для захисту даних

ISAKMP (Internet Security Association and Key Management Protocol – протокол TCP/IP стеку

L2TP (Layer 2 Tunneling Protocol) – протокол тунелювання другого рівня

MD5 (Message Digest 5) – алгоритм хешування

OSPF (Open Shortest Path First) – протокол динамічної маршрутизації

PKI (Public Key Infrastructure) – метод забезпечення криптозадач

RFC (Request for Comment) – документ Інтернету, що містить технічні стандарти

RSA (Rivest, Shamir, Adleman) – криптографічний алгоритм з відкритим ключем

SA (Security Association) – асоціація безпеки

SAD (Security Associations Database) – база даних асоціації безпеки

SHA (Secure Hash Algorithm) – алгоритм безпечного хешу

SMTP (Simple Mail Transfer Protocol) – протокол пересилання пошти

SOCKS (SOCKet Secure) – фреймова структура

SPD (Security Policy Database) – база даних політики безпеки

SPI (Security Parameters Index) – ідентифікаційний тег

SSH (Secure Shell) – мережевий протокол прикладного рівня

SSL (Secure Sockets Layer) – протокол безпеки на транспортному рівні

TCP (Transmission Control Protocol) – протокол передачі даних

TLS (Transport Layer Security) – криптографічний протокол

UDP (User Datagram Protocol) – протокол в стеку TCP/IP

ULP (Up-level protocol) – протокол верхнього рівня

VPN (Virtual Private Network) – віртуальна приватна мережа

ВСТУП

На даний момент нікого не дивує той факт, що рівень розвитку держави та суспільства в суттєвій мірі залежить та визначається рівнем їх інформатизації.

В наш час інформація стала найціннішим і найвагомішим об'єктом, у різних сферах життя, вона може привести до колосального розвитку ,так і стати причиною воєнного конфлікту. Саме тому інформація повинна бути захищеною, щоб зберегти свою цілісність, доступність і конфіденційність.

Завдяки всесвітньому Інтернету, людство отримало можливість передавати інформацію широко та інтенсивно в усі сфери життєдіяльності суспільства та держави, використовуючи новітні інформаційні, телекомунікаційні та інформаційно-телекомунікаційні системи.

При реалізації даних систем використовується різні програмні та програмно-апаратні методи, що намагаються у повній мірі надати захист переданим даним від злочинних дій третіх осіб. Розсекречення інформації впливає не тільки на людину, чиї дані були оприлюднені, але в масштабах держави порушення цілісності інформації стратегічних об’єктів впливає не лише на економічну сторону країни, а й несе наслідки негативного втручання на навколишнє середовище, безпеку держави і навіть на благополуччя суспільства. Тому захист інформації виходить на першочерговий рівень усіх відомств державного рівня[1].

На даний момент фахівці одноголосно визнають, що найнадійнішим методом захисту інформації від втручання є криптографічні методи. Даний спосіб відомий людству ще з давніх-давен, адже саме стародавнє суспільство внесло початок розвитку даного способу збереження даних.

Стрімкий розвиток комп’ютерної техніки призвів до посиленого розвитку криптографічних систем, що реалізовані в програмному та апаратно-програмному вигляді. Це дозволило вирішити безліч завдань, щодо збереження автентичності передачі даних по лініям зв’язку. Одним із важливих та пріоритетних завдань у даній сфері залишається не тільки розробка нових національних криптографічних систем і алгоритмів, що задовольняють сучасним технологічним вимогам, але й

підтримка криптосистем , що використовуються в цей час на відповідному рівні безпеки.

Отже, Метою кваліфікаційної роботи є підвищення захисту мовної інформації в мережі IP-телефонії на основі аналізу методів захисту інформації від несанкціонованого доступу, що можуть бути реалізовані навмисним впливом природного або штучного характеру.

Об’єктом є - процес функціонування в мережі IP-телефонії, предметом є - дослідження методи захисту інформації в мережі IP-телефонії.

РОЗДІЛ 1.
АНАЛІЗ ЗАГРОЗ В IP-МЕРЕЖІ

1.1 Аналіз міжнародного досвіду в області інформаційної безпеки

Стрімкий розвиток комп'ютерної техніки, що розпочався з середини XX століття, неодмінно зростає по експоненті. Людство, використовуючи все більше розумної техніки, крок за кроком підходить до нового етапу розвитку, що отримало назву «інформаційного суспільства».

Масове використання розумних технологій у всіх сферах діяльності людини та обсяг інформації, що зберігається на цих носіях, виріс в мільйони разів. На сьогоднішній день, нікого не вражає той факт, що майже 80% світової ринкової продукції складає результати розумової діяльності людини та обробка інформації. Саме тому, боротьба за світовий ринок поступово переходить з матеріального світу до віртуального простору, що призводить до проблем кібернебезпек та кіберзлочинності.

Комп'ютерні системи стали відкритими та вразливими до загроз, які стали популярними на даному етапі розвитку. Початковою проблемою використання Інтернет простору було не доопрацювання протоколу TCP/IP, що був створений перш за все для якісного та швидкого підключення техніки незалежно від їхньої операційної системи.

Зберігання інформації від несанкціонованого доступу не було основною метою розробників, що призвело до загальновідомих світових хакерських атак. На сьогоднішній день забезпечення цілісності та надійності роботи IT-мережі є основною метою, що відкидає простоту доступу на другий план.

Кіберзлочинці несанкціонованно проникають у комп'ютери, зламуючи системи великих підприємств, блокують доступ до даних, викрадають цінну комерційну інформацію, окрім переліченого, хакерські атаки на інтегрований простір створюють низку економічних проблем із довготривалими наслідками, що завдають серйозні негативні наслідки на рівні держави.

Експерти майже одноголосно підтверджують той факт, що на даний момент

збитки від хакерських зломів комп’ютерної системи сягають майже 500 мільярдів доларів кожен рік. Фахівці наголошують, що неможливо назвати реальні масштаби катастрофи кіберзлочинного шахрайста, адже дані надійно приховуються світовими компаніями для утримання власного рейтингу.

Комп’ютерна та мережева безпека важлива з таких причин:

- Захист активів компанії. Під «активами» мається на увазі захист безпосередньо інформації, що розміщується на комп’ютерах та електронних носіях та в мережі компанії. Інформаціє є головним об’єктом ураження. Інформаційна безпека націлена на захист цілісності, доступності та конфіденційності інформації.
- Для отримання конкурентної переваги: розробка та підтримка ефективної безпеки. Згідно з нормативними вимогами: співробітники компанії несуть відповідальність за забезпечення надійності організації. Згідно цього, компанії, що покладаються на комп’ютерні технології , повинні розробляти постійну політику, що необхідна не тільки для захисту комерційних даних, а також захистити компанію від відповідальності перед державою[5].

За результатами досліджень 2019 року «Лабораторії Касперского» було оприлюднено результати, що показують сучасну ситуацію нападів кіберзлочинців на підприємства по всьому світі. За даними аналітиків Китай залишається лідером за кількістю атак, що створюється. Часка атак у відсотковому показнику за 2018 рік виросла з 50,43% до 67,89%. Друге місце посідає США, хоча країна максимально зменшила свої показника в даній області з 24,90% до 17,17%. Детальніші результати досліджень виведено на рис. 1.1.

За вище згаданими даними можна зробити висновки про те, що найбільше злочинних нападів на інформаційні ресурси припадає на країни, що мають економічну, фінансову, технологічну незалежність і займають провідну роль у світі. Порушення цілісності інформації стратегічних об’єктів впливає не лише на економічну сторону держави, а й несе наслідки негативного втручання на навколишнє середовище, безпеку держави і навіть на благополуччя суспільства.

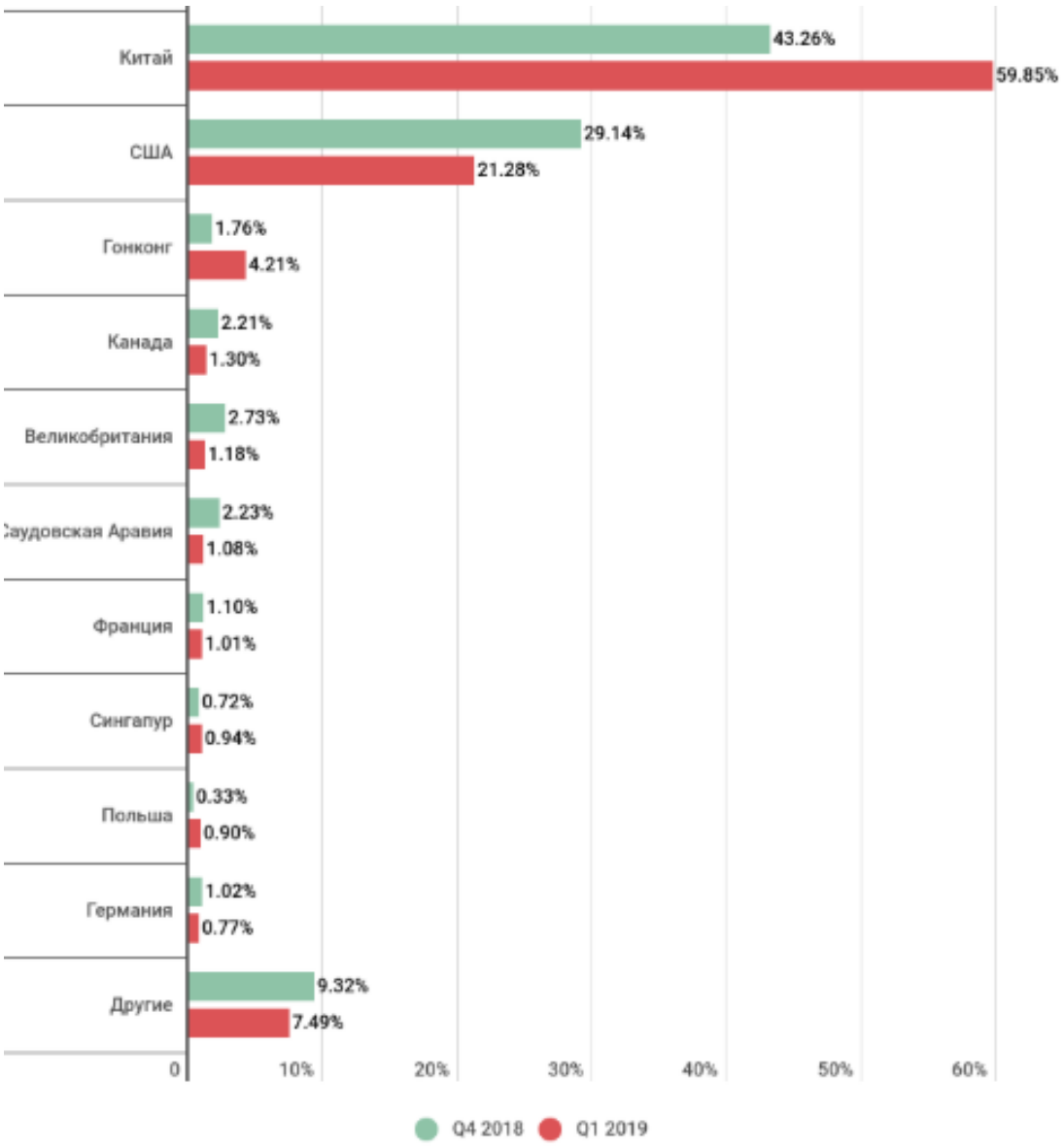

Рис. 1.1 Розподіл унікальних мішеней DDoS-атак по країнам, Q4 2018 року і Q1 2019 р.

1.2 Аналіз передумов виникнення загроз в IT-мережі

Головні економічні наслідки розкриття комерційної інформації хакерськими атаками на інформацію:

1. Втрата інтелектуальної власності
2. Усунення наслідків кіберзлочину
3. Втрата бізнес-інформації
4. Порушення цілісності роботи IT-мережи
5. Вартість забезпечення безпеки мережі

Якщо проблему захисту інформації та витоку даних розглядати з економічної точки зору, то загальний збиток інформаційної безпеки залежить від двох чинників: прямого і непрямого збитку. Прямий збиток виникає тоді, коли втрачається цілісність інформації внаслідок витоку. Відповідно непрямим збитком називають втрати, що зазнали підприємства внаслідок розповсюдження інформації, що відносять до конфіденційної. Загалом будь-яка втрата конфіденційних даних несе за собою низку економічних та фізичних наслідків, для усунення проблеми.

Проблема захисту інформаційних ресурсів виходить на державний рівень, адже дана тема торкається медичної, військової, дипломатичної, економічної сфери.

На сьогоднішній день рішення проблеми інформаційної безпеки вже розглядаються на державному рівні, що підтверджується нормативно-правовими і організаційними документами. В Україні на цей час діє три Закони України: «Про електронні документи і електронний документообіг» , який встановлює основні організаційно-правові принципи електронного документообігу і використання електронних документів; «Про електронний цифровий підпис», який визначає правовий статус електронного цифрового підпису та регулює взаємовідносини, які виникають при використанні електронного цифрового підпису та Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», що регулює взаємовідносини в області захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах[1-2].

Забезпечення безпеки інформаційних технологій являє собою комплексну проблему, яка охоплює правове регулювання використання ІТ, удосконалення технологій їх розробки, розвиток системи сертифікації, забезпечення відповідних організаційно-технічних умов експлуатації.

Держава першочергово має проаналізувати потенційні загрози на безпеку інформаційних ресурсів та можливі наслідки розкриття інформації, підрахувати збитки і витрати на реалізацію захисту.

У межах моєї роботи під загрозою розкриття інформації будемо розуміти такий стан, коли отриманий несанкціонований доступ до ресурсів, при чому йдеться

як про відкриті, такі і ті ресурси, які мають обмежений доступ. Ці ресурси мають передаватися один одному і зберігатися у єдиній інформаційній системі.

Особливої гостроти дана проблема набуває у зв'язку з масовим використанням Інтернет-технологій, що призводить до масового витоку персональних даних технічними каналами. Під витоком персональних даних розуміється неконтрольоване поширення персональної інформації, яке призводить до її несанкціонованого одержання третіми особами, що не мають на неї права[4].

Витік інформації відбувається відповідним каналом витоку. Оскільки засоби розвідки противника, як правило, технічні, то і канали витоку також називають технічними. На рис. 1.2 структурно зображено технічний канал витоку інформації.

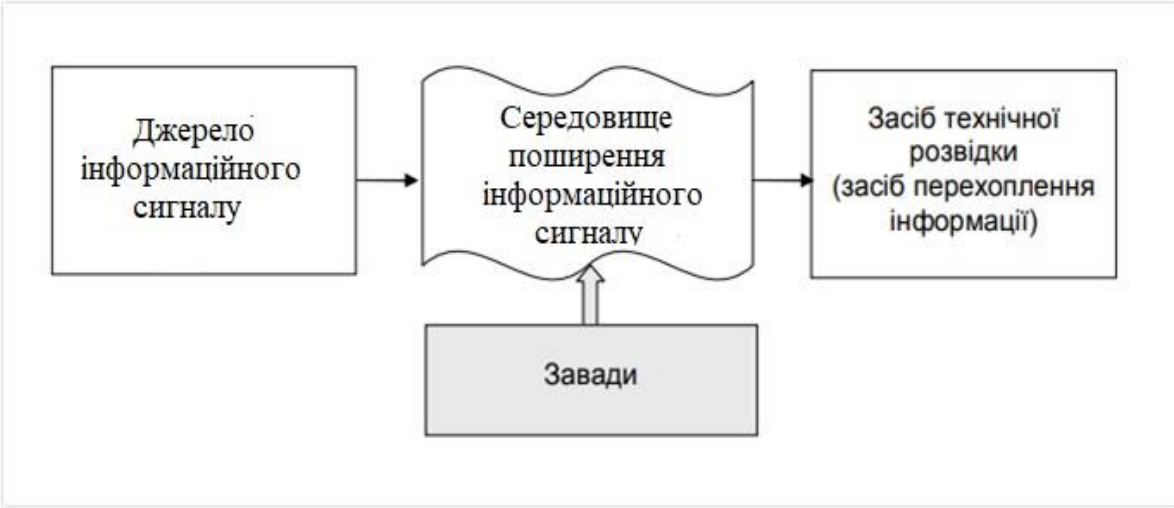

Рис. 1.2 Технічний канал витоку інформації

З цього випливає, що існує така інформація, яка потребує захисту. Захист інформації – це безпосередньо сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації.

Класифікувати інформацію можна за такими видами, що схематично представлено на рис. 1.3.

Рис. 1.3 Класифікація інформації за режимом доступу

- Відкрита – містить примітивні відомості про об’єкти та безпосередньо оброблює базові поняття, зрозумілим більшій частині суспільства.

Інформацією з відкритим доступом має бути надана усім користувачам для ознайомлення. Такі функції як редагування, модифікація, повне знищення можуть здійснювати лише аутентифіковані об’єкти, яким надані певні повноваження, а неавторизованим користувачам, або користувачам з не підтвердженою під час аутентифікації відповідністю повинні блокуватися.

- Інформація з обмеженим доступом – вид даних, який містить специфічний набір понять, доступ до якої обмежений у рамках вузької соціальної групи, для якої дана інформація має значення. Така інформація поділяється на конфіденційну та таємну. Інформація таємна (secret information) – інформація з обмеженим доступом, що містить відомості, які становлять державну та іншу передбачену законом таємницю і розголошення яких завдає шкоди об’єктам державного значення. Інформація конфіденційна – інформація з обмеженим доступом, що містить відомості, які перебувають у володінні, користуванні чи розпорядженні окремих фізичних чи юридичних осіб або держави, і порядок доступу до якої встановлюється ними[2].

Доступ до службової інформації надається тільки ідентифікованим та аутентифікованим користувачам. Спроби доступу до такої інформації неідентифікованих осіб чи користувачів з не підтвердженою під час аутентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.

У системі забезпечується можливість надання користувачеві права на виконання однієї або кількох операцій з обробки конфіденційної інформації або позбавлення його такого права.

1.3 Класифікація основних видів загроз в мережі IP-телефонії

В залежності від класифікації інформації можна виділити основні види атак:

1. Вандалізм, з метою отримання інформації для власного користування або для самоствердження.
2. Кримінальні атаки, з метою отримання персональних даних малих підприємств, фірм.
3. Шпіонаж(розвідка) з метою отримання інформації, що належить державі.

На сьогоднішній день вчені виділяють шість основних загроз інформаційній безпеці, а саме:

1. Розкриття конфіденційної інформації
2. Злом (неправомірне втручання в роботу комп’ютерної системи)
3. Виведення системи з ладу, зниження її працездатності
4. Перевищення повноважень непривілейованим користувача
5. Знищення та спотворення інформації

Якщо розібратись конкретніше, то можна досить чітко дати визначення для інформаційної безпеки:

Інформаційна безпека = конфіденційність + цілісність + доступність.

З цього випливає, щоб інформація була у повній мірі переданою правильно, і дійшла до кінцевого пункту призначення у повному обсязі, потрібно обов’язково підтримати її характеристики.

У широкому спектрі загрози на інформаційні ресурси можна розглядати як можливі випадки природного, штучного, та антропогенного походження, що можуть привести до небажаного впливу на інформаційні ресурси, та інформацію, що знаходиться в ній. Несприятливий вплив на елементи інформаційної системи можна охарактеризувати, як уразливість системи. Саме через цей показник відбувається активізація загроз.

З різних способів класифікації загроз даних, базовою є класифікація за наслідками впливу на інформацію. Захист інформації ведеться з метою підтримки таких властивостей інформації як:

1. Погроза порушення конфіденційності інформаційним ресурсам
2. Порушення цілісносності інформації
3. Порушення дієздатності інформаційно-обчислювальних систем

Розглянемо більш конкретніше ці властивості.

Загроза конфіденційності інформаційних ресурсів полягає у тому, що дані, стають розкритими, тобто персональні дані стають відомими особам, що не мають повноважень доступу до неї.

Загроза порушення цілісності інформаційних ресурсів полягає в навмисному антропогенному впливі на дані, що зберігається в обчислювальній системі чи переданої з однієї системи в іншу.

Порушення дієздатності інформаційно-обчислювальної системи виникає щоразу, коли в результаті навмисних дій, що вживаються іншим користувачем або зловмисником, блокується доступ до деякого ресурсу обчислювальної системи.

Насправді блокування обчислювального обладнання може бути постійним, тому щоб ресурс, що запитується, ніколи не був отриманий, або може викликати затримання в отриманні ресурсу, що запитується, що є достатнім для того, щоб він став некоректним.

Розглянемо класифікація можливих загроз безпеки інформаційних систем за такими ознаками:

1. По природі виникнення виділяють:

- природні загрози, викликані впливом фізичних процесів чи стихійних природних явищ;
- штучні загрози, спричинені рукодіянням людини.

Найбільш частими та небезпечними є ненавмисні помилки, що спричинені антропогенними чинниками. Загалом, було проведено дослідження вченими, що спеціалізуються на інформаційній безпеці та захисту інформації, понад 67% помилок є наслідком ненавмисних помилок, що у порівнянні з природними, наприклад, повені, землетруси, пожежі, трапляються набагато рідше.

2. По ступеню навмисності виділяють:
- загрози, викликані помилками і недбалістю;
- умисні загрози.

Наступними розглянемо такі критерії, як навмисні крадіжки та халатність. Майже у всіх випадках, об'єктами вчинення даних дій були працівники організацій, які добре знають роботу інформаційної системи та критерії взлому. Згідно статистики, що була оприлюднена журналом: "Control Systems and Computers", 80% працівників навмисно наносили шкоду фірмі, в якій вони працювали, через образу і тільки 20% дій були спричинені невідповідальною роботою. Навмисне пошкодження може знайти відображення у наступних діях:

- пошкодження обладнання;
- налаштування бомби, що створена для руйнації програмних додатків;
- введення недоцільних даних;
- модифікація даних;
- надання доступу до даних із обмеженим доступом тощо.

Підприємцям варто обов'язково слідкувати за тим, щоб після звільнення підприємців його права доступу до використаних ресурсів було закрито та змінено паролі доступу.

3. По джерелу загроз виділяють:
- природне середовище;
- людина;
- ліцензійні програмні засоби;

- неліцензійні програмно-апаратні засоби.

Головною загрозою цілісності інформації становлять зловмисні програмні та програмно-апаратні додатки, що суттєво зменшують продуктивність, впливають на швидкість та стійкість системи. Розглянемо на прикладі рис. 1.4. потенційно небезпечні додатки.

Рис. 1.4 Потенційно небезпечні програмно-апаратні загрози безпеці

Якщо брати до уваги хакерські атака, які реалізуються щодня то у порівнянню з програмними вірусами вони не складають великого відсотку шкоди. Вірусні програми здатні розповсюджувати свої копії на величезну кількість комп'ютерів по каналам зв'язку за короткий термін, що призводить до порушення функціональної частини операційної системи та витоку інформації.

Щоб максимально захистити свої дані власники підприємств готові наймати спеціалістів в даній області, щоб уникнути витоку інформації через програмно-апаратні збої.

4. По мірі впливу на інформаційну систему, виділяють:

- пасивні загрози;
- активні загрози.

Пасивна загроза у даному випадку не несе серйозної шкоди апаратній частині системи, вона лише має вплив на конфіденційність переданої інформації.

Активна загроза навпаки призводить до зміни комп'ютерної системи, що несе за собою втрату інформації і порушення дієздатності системи, яку потрібно відшкодовувати матеріальним чином.

5. За місцем розташування інформації, що зберігається та опрацьовується в інформаційній системі розрізняють:

- загрози доступу до інформації яка розташована на зовнішніх пристроях зберігання інформації;
- загрози доступу до інформації в ОП;
- загрози доступу до інформації, що проходять по каналам зв'язку;

6. За ймовірністю реалізації:

- ймовірні;
- неможливі;
- випадкові.

7. За етапами доступу користувача розрізняють:

- загрози, що проявляються на етапі доступу до ресурсів;
- загрози, що проявляються після етапу доступу до ресурсів.

Інформаційну безпеку слід розглядати як спектр, що має пропорційно гарантувати захищеність. Захист має бути пропорційний загрозі, що виникає і лише тоді можна говорити про цілісність системи захисту інформації[8-9].

Наведена класифікація наочно демонструє різностороння та несхожість загроз та небезпек інформаційній безпеці, які є адекватними часу і простору, темпам розвитку суспільства.

На сьогоднішній день однією із причин вразливості інформаційної системи є те, що інформація знаходиться на різних носія і має хаотичне територіальне

розміщення. Наприклад, персональні дані можуть розміщуватись як на зовнішніх пристроях накопичування так і на внутрішніх, наприклад, персональний комп'ютери, мобільні телефони, магнітні оптичні носії, карти пам'яті та ін. У деяких випадках носієм даних також може розглядатися людина.

Втрата інформацією своєї автентичності може статися внаслідок переміщення з одного пристрою на інший або фізичні зміни носія. В таких умовах важливість правильної побудови захисту інформації на цих носіях в край важлива. Але є деякі труднощі у реалізації:

- відсутність єдиної теорії і методології захисту персональних даних на різних носіях;
- для реалізації методології захисту потрібно розробити технічні та логічні проблеми;
- створення відповідної документації.

Щоб максимально ефективно розробити план подолання даних проблем, необхідно розробити відповідні стратегічні координаційні дії рівні держави. Професіонали у даній сфері розробили концепцію захисту інформації від несанкціонованого доступу, що рекомендують розгортати в три етапи.

Під поняттям «концепція захисту інформації» будемо розуміти систему поглядів на проблеми в захисті інформації та стратегію вирішення даних негараздів за допомогою сучасних методів рис. 1.5.

Розробку концепції захисту представлено на рис. 1.6, яка має три головні етапи розгортання.

Рис. 1.5 Схема представлення стратегії захисту інформації

Рис. 1.6 Схема етапів концепції захисту інформаційних ресурсів

На першому етапі обґрунтоване цільове значення інформації, яка потребує захисту, тобто проводиться повний збір інформації та проводиться аналіз об’єкта. Відповідно на другому етапі розглядаються можливість виникнення реальних проблем та загроз, що можуть вплинути під час зберігання інформації. Заключним етапом є проведення обґрунтування методів захисту інформаційних ресурсів, тобто

створення відповідних технічних, логічних заходів для створення максимальної безпеки з використанням економічних ресурсів.

Домогтися високого ступеня захищеності можна тільки при використанні передових технологій захисту мережі передачі даних. У міру розвитку і ускладнення засобів, методів і форм автоматизації процесів обробки інформації підвищується і рівень загроз для використовуваних інформаційних технологій. З кожним роком з'являються все нові і нові атаки на мережі передачі даних. У відповідь на нові атаки з'являються нові або вдосконалюються старі методи захисту інформації та інформаційно-технічної інфраструктури.

Повністю захистити інформацію неможливо, тому технології захисту даних ґрунтуються на застосуванні сучасних методів, які запобігають перехоплення інформації та її втрати. На сьогоднішній день найкращим способом зберегти цілісність даних є криптографічні методи захисту інформації із використанням шифрування, що реалізується в програмному або програмно-апаратному вигляді.

Ця обставина, обумовлена масовим застосуванням криптографічних методів і різноманітністю завдань, що розв'язуються з їх допомогою, приводить до істотного підвищення вимог до стійкості сучасних криптосистем, технологічності процесів їхньої розробки й проектування, економічності їхніх реалізацій. Одним із важливих та пріоритетних завдань у даній галузі залишається не тільки розробка нових національних криптографічних систем і алгоритмів, що задовольняють сучасним технологічним вимогам, але й підтримка криптосистем , що використовуються в цей час на відповідному рівні безпеки.

Висновки:

На сьогоднішній день відома велика кількість загроз інформації, які можуть бути реалізовані навмисним впливом природного або штучного характеру, що можуть завдавати збитки суб'єктам інформаційних відносин.

Загрози – це внутрішні чи зовнішні втручання, які можуть порушити функціонування, цілісність та автентичність мережі. Окрім визначених загроз, можливі недоліки в проектування корпоративної мережі, а саме, вразливості

обладнання, програмного забезпечення, фізичні, людський фактор, перехоплення інформації, неконтрольований доступ до медіа-ресурсів.

Відповідно, захист конфіденційності інформації від небажаного втручання дуже відповідальна та актуальна задача на сьогоднішній день, адже, якщо мережа зв'язку побудована з використання всіх можливих сучасних методів захисту інформації, то з логічної точки зору неправомірні дії злочинців не можуть нашкодити цілісності та дієздатності даної системи. Але це не зовсім так.

Отже, можна зробити висновки, що жодна захищена система не здатна довгий час протистояти навмисним діям кіберзлочинця. Завданням захисту інформації полягає у тому, щоб шахраї якомога довше не змогли завдати шкоди системі зв'язку, саме для цього потрібні все більше новітніх методів і алгоритмів збереження даних.

РОЗДІЛ 2.
ОЦІНКА СПОСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В ПАКЕТНИХ МЕРЕЖАХ ЗВ'ЯЗКУ

2.1 Способи побудови системи захисту інформації в IP-телефонії

Завдяки масового використання комп'ютерної техніки для передачі даних та інформації попит на швидкість та надійність зріс у декілька разів. Суспільство задумалось про можливості передачі даних на великі відстані за допомогою Internet з'єднання, що мало підтримувати ці критерії. Однак критерії побудови Internet мережі не є максимально захищеною, що робить її уразливою для будь-яких несанкціонованих атак.

Гарантом безпеки також важко назвати мережі, що створені на основі протоколів TCP/IP, UDP/IP і звичайних Інтернет додатків, якими ми користуємось кожен день.Порушення дієздатності мережі виникає щоразу, коли в результаті навмисних дії третіх осіб, що вживаються іншими користувачами або зловмисниками, блокується доступ до деякого ресурсу обчислювальної системи.

На даному етапі вчені виділяють шість основних способів захисту мережі, що створюють перепони на шляху зловмисників: перешкода, маскування, регламентація, управління, примус, спонукання[12]. Всі вище перераховані методи націлені на побудову ефективної мережевої технології захисту інформації, при якій виключені втрати через недбалість.

Для безпечного використання відкритих мереж використовують метод віртуально захищених мереж VPN (Virtual Private Network). Одним із ключових критеріїв є те, що дана мережа будується без участі телефонної лінії, а безпосередньо з використанням Internet-мережі і діючої IP адреси, що на даний момент відповідає всім критеріям швидкості передач даних.

Рис. 2.1 Загальна схема VPN

Суть технології віртуальних приватних мереж полягає в тому, що при підключенні до VPN сервера за допомогою спеціального апаратно-програмного забезпечення поверх загальної мережі, що використовується, у вже побудованому з'єднанні створюється зашифрований канал, що забезпечує високий рівень захисту каналу інформації від небажаного втручання третіх осіб. Таким чином, створюється "тунель" між персональним комп'ютером і сервером, в якому всі дані зашифровані, і провайдер не розуміє, з яким сайтом працює користувач. Ключовим критерієм VPN технології являється її безпосередній захист корпоративної інформації, що передається по відкритим лініям передачі, які мають бути надійно захищені криптографічними методами.

З технічної точки зору реалізація віртуального приватного тунелю можна представити так:

1. Технологія, що забезпечує недоторканий вигляд даних, що передаються, на основі побудови з’єднань (frame relay або ATM) між двома точками, до яких не мають доступи інші користувачі.

2. Технологія «Тунелю», що дозволяє створювати віртуальні канали[4].

У 2001 році стався ринковий переворот у використанні даних технологій через збільшення мобільних пристроїв, що поступово посунув використання frame relay на

другий план і дав можливість стрімкого розвитку IP VPN, через його суттєву економію використовуваного каналу зв’язку.

Одним словом, технологія VPN дуже складна, вона побудована за допомогою комунікаційних технологій, криптографічних методів, технологій авторизації на аутентифікації. Тунельна технологія є ключовою технологією для налаштування мережі VPN.

Дана технологія інкапсуляції вирішує проблему великої кількості ресурсів, адже дає можливість організувати безпеку не тільки окремим підрозділам, а захистити від несанкціонованих зломів всю мережу.

Одним словом, технологія VPN дуже складна, вона побудована за допомогою комунікаційних технологій, криптографічних методів, технологій авторизації на аутентифікації. Тунельна технологія є ключовою технологією для налаштування мережі VPN.

На даному етапі розвитку розумних технологій все більше компаній, державних установ, філій звертаються до побудови віртуальних мереж за допомогою VPN, відкидаючи на другий план з’єднання за допомогою модемів, що раніше використовувалась для побудови з’єднань між користувачами Internet. Популярність дана технологія набуває через її економічність та малозатратність в порівнянні з іншими технологіями. З'єднання з сервером через VPN має ряд переваг:

1. Створення WAN-з’єднання дуже дороге і може бути недоцільним для окремих користувачів. Дані, що передаються між двома кінцевими точками VPN, зашифрована, таким чином, жодне несанкціоноване втручання неможливе, коли інформація передається мережею загального користування.
2. Приховування конфіденційності, маскування дійсної IP-адреси.
3. Обходження географічних обмежень[5].

2.2. Оцінка технології для захисту від несанкціонованого доступу

Базовою частиною VPN-технології на основі Internet являються дві основні технології такі як:

1. Технологія «тунелю» (tunneling) або так звана інкапсуляція (encapsulation).

2. Технології, які надають конфіденційності і цілісності інформації, що передається, а також її автентифікацію та авторизацію користувачів, які мають безпосередньо доступ до неї (аутентифікація та шифрування).

На даному етапі розглянемо детальніше технологію «тунелювання» - це спосіб передачі даних через проміжну мережу. Дана технологія використовується не тільки для забезпечення конфіденційності внутрішнього пакета даних, але і для його цілісності, але без додаткового захисту тунельні технології не дуже безпечні. Коли мережеві атакуючі успішно атакують VPN, використовуючи слабкість безпеки тунельних протоколів, вся безпечна передача даних з використанням технології VPN в Інтернеті перестає бути надійною.

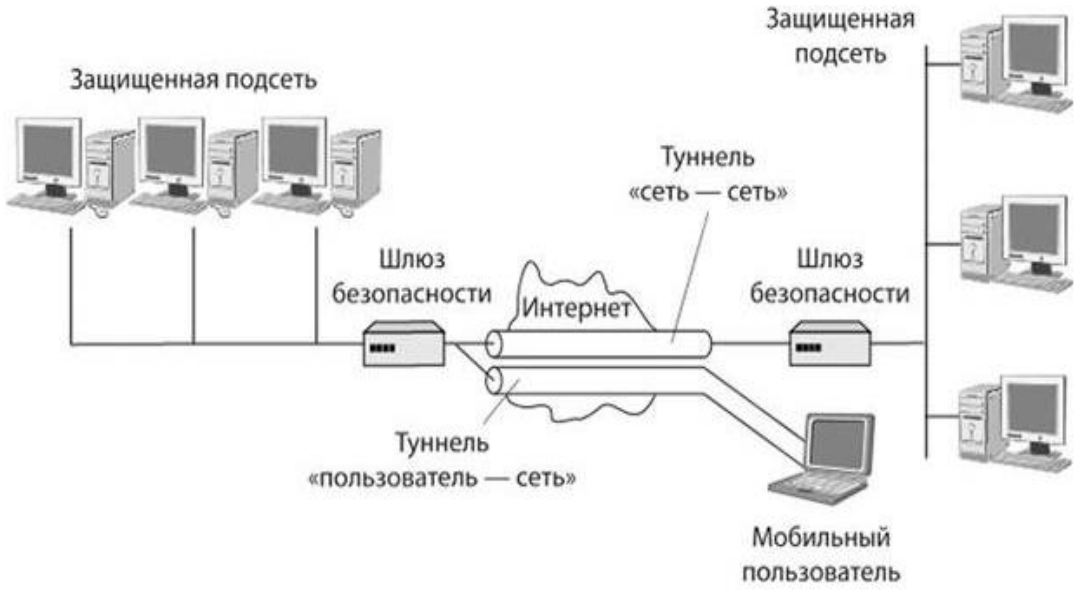

Рис. 2.2 Тунельна схема організації VPN-мережі

Дані проблеми вирішуються криптографічними методами. Щоб передані дані дійшли до кінцевої точки без змін, використовують метод електронного цифрового підпису(ЕЦП). До інформації, що передається додається додатковий блок даних побудованих за допомогою криптографічних алгоритмів, що можна дешифрувати лише за наявності особистого ключа, що проходить перевірку через відкритий ключ.

Отже, простими словами в процесі тунелювання дані розбиваються на більш дрібні пакети, які потім будуть переміщатися по "тунелю" для транспортування до кінцевого пункту призначення. Перед тим як потрапити в Internet-тунель дані шифруються сильними криптографічними алгоритмами, що забезпечує їх додатковий захист та надійність. Загалом з використанням Internet VPN швидкість передачі даних стала економічно вигіднішим рішенням, тому підприємства можуть більше не використовувати дорогі Intanet, Extranet мережі.

Щоб створити безпечну передачу даних по каналам Internet потрібно ефективно вирішити дві головні задачі:

1. Безпечне підключення до відкритих мереж від несанкціонованих дій з боку зовнішнього середовища
2. Збереження автентичності даних, що передаються по відкритому середовищу мереж

Для захисту локальных мереж від несанкціонованого доступу використовують програму firewall, але користувачі частіше називають її брандмауером. Дана програма використовується у ролі так званого «фільтра», що відслідковує з’єднання комп’ютерів, аналізує з’єднання, що створилося і виносить рішення чи надавати йому дозвіл на роботу чи ні. Брандмауер умовно можна поділити на дві підпрограми - персональну та корпоративну.

Під персональною розуміється програма, що налаштовується на персональний комп’ютер, а корпоративний firewall налаштовується адміністратором на шлюз між Internet та локальною мережею, що і надає надійний захист від зловмисників.

Для захисту приватного мережевого трафіку через незахищені відкриті мережі використовують VPN канал. Дана технологія забезпечує криптографічне шифрування приватного трафіку. Інформація, що передається по таким каналам зв’язку, шифрується, а пакети майже неможливо перехватити без правильно підібраних ключів шифрування. VPN-Internet дає можливість віддалено працювати і використовувати корпоративний сервер і безпечно передавати конфіденційну інформацію через Internet[12-13].

Реалізувати віртуальну приватну мережу можна різними методами. Головною метою вибору способу побудови є її продуктивність та швидкість, сумісність між сайтами і компаніями, а також необхідність підтримувати багато типів мережевих профілів зв'язку, адже неправильна побудова може зупинити роботу мережі, через малопотужність маршрутизаторів, технічні конфлікти, політичні проблеми і проблема технічного досвіду, пов'язаними з будь-яким рішенням тому найкраще використовувати спеціалізоване обладнання або програмне рішення.

Основними способами реалізації VPN є:

1. Remote access VPN
2. Site-to-site VPN

Шлюзи захищеного віддаленого доступу (Remote Access VPN) - це програмно-апаратні або програмні забезпечення, які надають можливість захищеного підключення користувачів до ресурсів корпоративної мережі через Інтернет та інші відкриті мережі. Remote Access VPN реалізовує захищену мережу за принципом "мережу - віддалений користувач"[6].

Шлюзи захищеного віддаленого доступу налаштовуються на кордон мережі, а на віддалених персональних пристроях користувачів, що мають доступ до мережі Internet,налаштовуються програмно-апаратні VPN.

Саме реалізація за допомогою VPN з мережею "мережа - віддалений користувач" відповідає за криптографічний захист, шифрування та дешифрування даних, що передаються.

З точки зору використовуваних протоколів можна виділити кілька типів Remote Access VPN:

- використовують протоколи сімейства IPSec / IKE;
- використовують протоколи сімейства SSL / TLS;
- використовують неліцензійні та незареєстровані протоколи, що несумісні з іншими рішеннями.

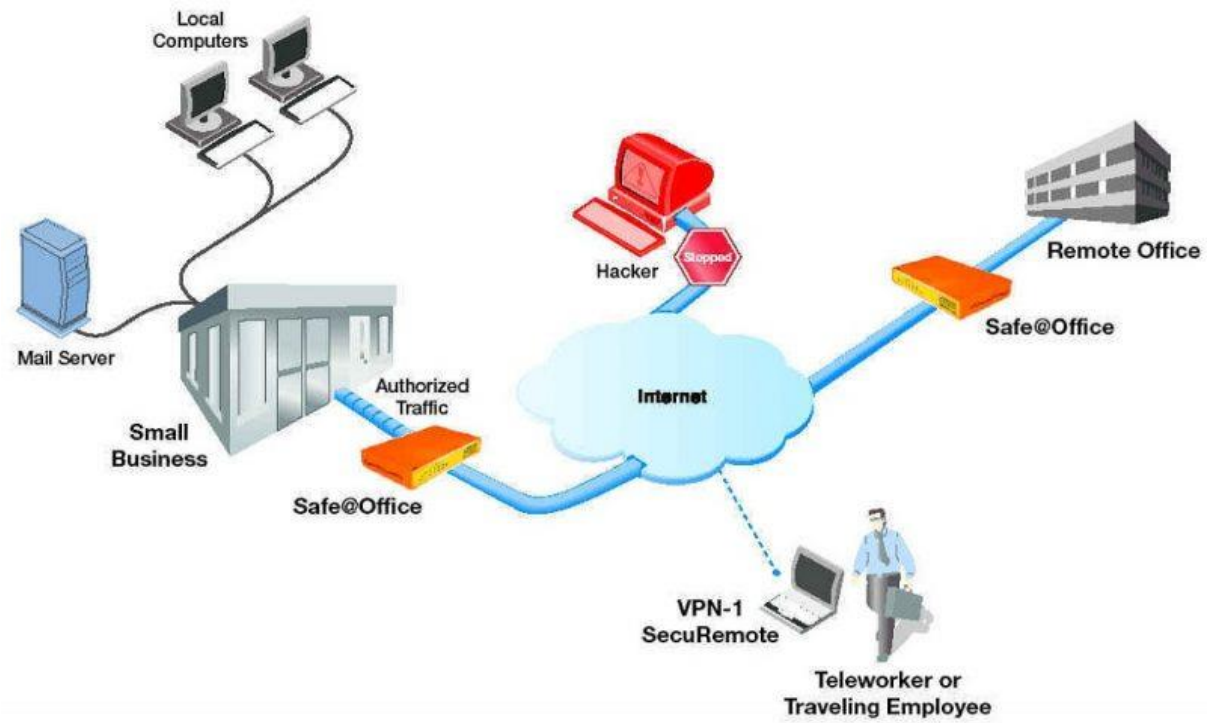

Рис. 2.3 Загальна схема підключення Remote access VPN

Для побудови захищеної мережі за принципом "мережа - віддалений користувач" потрібен шлюз VPN для автентифікації пристроїв, що авторизується у VPN або NAS -сервер для зберігання даних на файловому рівні. За правилами Remote access VPN має бути пристрій, що має клієнтське програмне забезпечення. Таким чином, ПЗ користувача VPN з'єднується із шлюзом VPN для автентифікації пристроїв(віддаленого користувача) та створює VPN тунель між локальною мережею та шлюзом[18].

Дані, що передаються спочатку переобразуються та шифруються VPN з віддаленим доступом, а вже тоді преедається на шлюз, що розташований поза локальною мережею. Після надходження даних до шлюзу, вони підлягаються дешифруванню і ретрансляції в локальну мережу.

Site-to-site VPN – реалізація в локальних мережах захищеного тунелю за допомогою двух маршрутизаторів для передачі даних без використання програмного забезпечення.

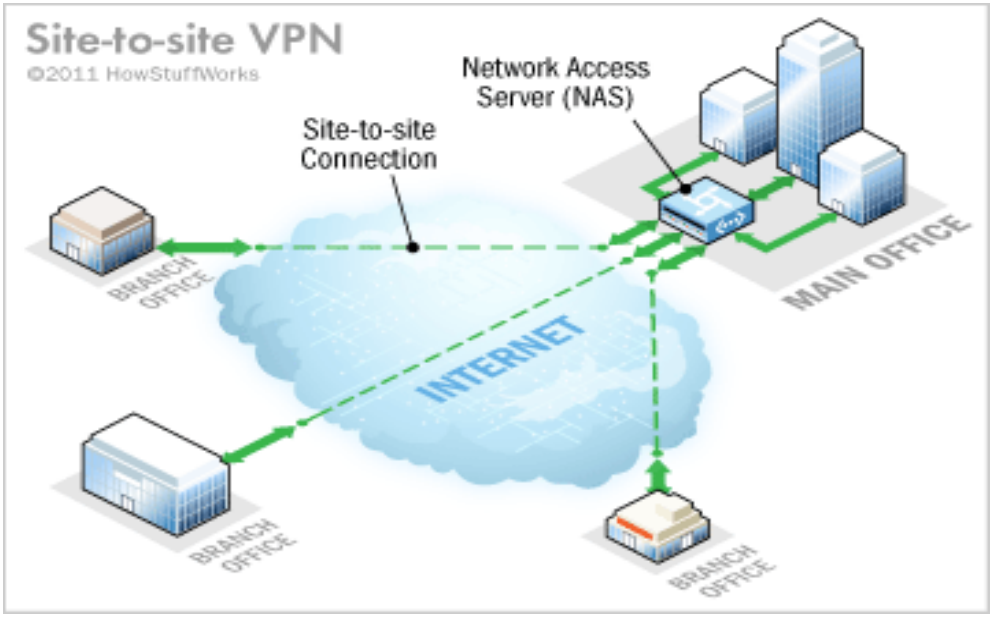

Рис. 2.4 Технічна реалізація VPN site-to-site

VPN site-to-site налаштовують для збільшення мережі однієї фірми на кілька офісних міст. Існує два поширені типи VPN від сайту до сайту: інтранет та екстранет. Внутрішні мережеві VPN на базі внутрішньої мережі використовуються для об'єднання локальних мереж декількох офісних локацій в одну приватну мережу, яка б тоді була відома як WAN (Wide Area Network). З іншого боку, VPN, що базуються на екстранеті, дозволяють компанії використовувати загальнодоступний Інтернет для підключення своєї локальної мережі до мереж інших фірм. Це надає змогу пересилати дані з інших будівель, зберігаючи свою локальну мережу (intranet)[7].

Класифікувати VPN-технологію можна за різними технічними критеріями: по ступеню захищеності, по способу реалізації, по призначенню, а також по рівню роботи в моделі OSI.

За типом захищеності використовуваного середовища VPN можна поділити на захищені та довірчі. Перші у свою чергу створюють надійний канал передачі пакетних даних, створюючи надійну підмережу на основі незахищеної мережі. Популярними захищеними приватними мережами можна вважати IPSec, OpenVPN і PPTP. Довірчі протоколи, такі як MPLS і L2TP у свою чергу дозволяють зашифрувати мультипротокольний трафік з іншими протоколами, наприклад, в парі з IPSec, забезпечуючи надійну безпеку.

Рис. 2.5 Класифікація VPN

Класифікація рішення VPN по призначенню:

1. Intranet VPN
2. Remote Access VPN
3. Extranet VPN
4. Client / Server VPN
5. Internet VPN

Intranet VPN дозволяє створити надійні з'єднання між внутрішніми підрозділами розподіленої компанії. Для такої мережі маються на увазі: криптографічні засоби захисту інформації, надійність роботи важливих додатків, електронної пошти, швидкість і продуктивність передачі.

Remote Access VPN дозволяє створити захищений канал між сегментом корпоративної мережі (центральним офісом або філією) і єдиними користувачами, що мають доступ до корпоративного ресурсу за допомогою персонального комп'ютера.

Extranet VPN дозволяє створити захищену від несанкціонованого доступу корпоративну мережу, що використовує Інтернет-технології для внутрішньокорпоративних цілей.

Client / Server VPN технологія надає захист даних, що передаються між двома вузлами корпоративної мережі. Особливість полягає в тому, що VPN будується між

вузлами, що перебувають, як правило, в одному сегменті мережі, наприклад, між робочою станцією і сервером.

Internet VPN технологія дозволяє створити «тунель» для передачі даних, що дозволить зберегти цілісність та автентичність інформації.

У моїй дипломній роботі я буду розглядати саме рішення VPN на базі Internet, що має більшу доступність і використання на даний момент. Саме це рішення є більш економічним та має суттєву перспективу.

2.3 Аналіз сучасних методів захисту інформації на основі криптографічних методів

Протоколи тунелювання VPN пропонують різні функції і рівні безпеки, і кожен з них має переваги і недоліки. Розташування VPN-технології тісно пов'язана із моделлю OSI, в якій присутні чіткі ієрархічні взаємозв'язки. Кожен рівень може вміщувати протоколи, які потім реалізують службу, що в свою чергу виповнює відповідну функцію і передає дії наступному рівню.

Рис. 2.6 Основні рівні моделі OSI, які використовуються для побудови мереж VPN

Саме від рівневого розташування залежить функціонал і сумісність з різними додатками і службами захисту нашої VPN-мережі.

Розглянемо детальніше протоколи канального рівня моделі OSI. Основними протоколами шифрування на даному рівні виступають L2TP і PPTP, які надають конфіденційності інформації через автентифікацію авторизацію.

Цей документ визначає протокол, який дозволяє туннелювання протокола точка-точка (PPP) через IP-мережу.

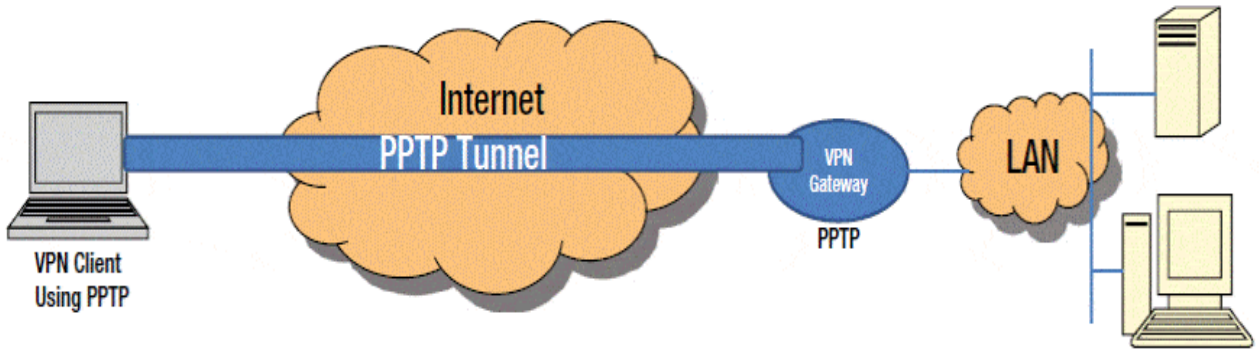

Рис. 2.7 Реалізація протоколу (PPP)

На даний момент досить популярним є протокол «точка-точка» або так званий Point-to-Point Tunnelling Protocol, що працює на TCP-порту. Даний протокол був створений ще в кінці 90-х років, для інкапсулювання протоколу PPP. Хоча даний протокол і має позитивні характеристики такі як швидкодія, доступність, простота реалізації і підтримується майже на всіх пристроях із низькою продуктивністю, все ж таки він має серйозні недоліки.

PPTP дозволяє шифрувати мультипротокольний трафік і потім обернути його в заголовок, який буде відправлений через мережу з використанням IP.

Протокол «точка-точка» використовує підключення через стек протоколів TCP/IP. PPTP використовує з'єднання протоколу управління передачею для управління тунелями та інкапсуляції загальної маршрутизації для перенесення кадрів PPP для даних, які передаються тунелем. Дана побудова створює приватну мережу, але в даній структурі виникають негаразди з боку шифрування та захищеності даних[8]. Іншим не менш важливим негараздом є використання протоколу «точка-точка», для створення безпеки.

Розглянемо детальніше роботу протоколу PPTP з інкапсульованим пакетом даних для передачі по IP-мережі. На рис. 2.8 приведена структурна схема пересилки даних по тунелю PPTP.

Рис. 2.8 Схема пересилки даних по тунелю PPTP

PPTP дає можливість реалізувати захищений канал для передачі службових пакетів по протоколам IP. Дані, що передаються спочатку переобразуються в кадри PPP, потім інкапсулюються по протоколу PPTP в пакет GRE, після чого у вже зашифрованому вигляді передаються через мережу. Для створення належної безпеки передачі даних протокол PPTP створює з'єднання для керуванням тунелем, адже GRE не може належним чином забезпечити безпеку. Лише після створення інкапсульованого GRE пакету виконується інкапсуляція в IP пакет. Комп'ютер-відправник надсилає дані через віртуальний тунель. Компютер-отримувач видаляє всі службові заголовки, залишаючи лише дані PPP.

Рис. 2.9 Архітектура протокола PPTP

PPTP можна використовувати для віддаленого доступу і VPN-з'єднань «точка-точка». При використанні Internet PPTP-сервер є VPN-сервером з підтримкою PPTP з одним інтерфейсом в Internet і другим інтерфейсом в корпоративній інтрамережі.

Недоліком протоколу PPTP є його побудова лише в IP-мережі і для створення віртуального тунелю для передачі пакетів потрібне окреме з'єднання. Тому раціонально використовувати протокол L2TP, що у комбінувані з IPSec створюють

належну надійність даних у повірянні з PPTP. L2TP вважають одним із найперспективніших протоколів для побудови захищених каналів.

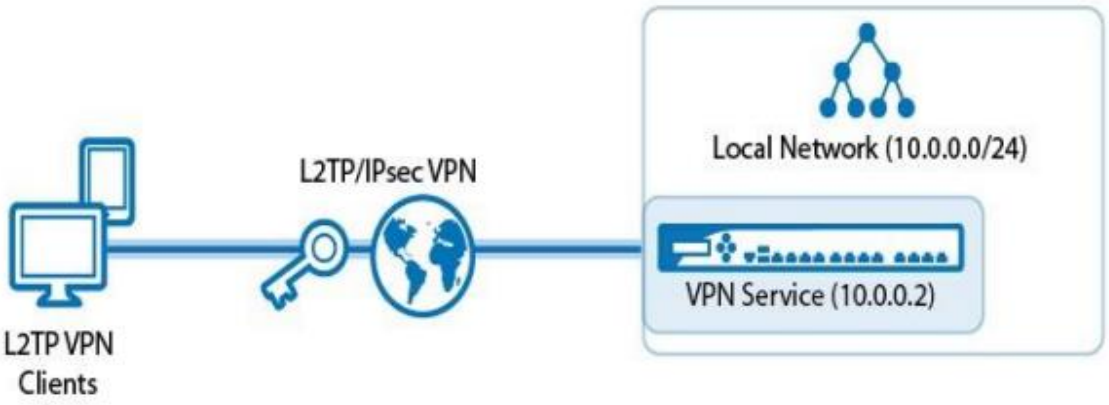

Рис. 2.10 Структурна схема побудови тунелю на канальному рівні

L2TP це комбінація PPTP і Layer 2 Forwarding (L2F). L2TP представляє кращі функції PPTP і L2F[9]. На відміну від PPTP, L2TP покладається на IP- безпеку (IPsec) в транспортному режимі для служб шифрування.

L2TP дозволяє зашифрувати мультипротокольний трафік, а потім використовувати будь-який носій, що підтримує доставку даних PPP, наприклад, IP або асинхронний режим передачі. Комбінація L2TP і IPsec відома як L2TP / IPsec.

PPP кадри	
L2TP інформаційні повідомлення	L2TP управляючі повідомлення
L2TP інформаційний канал (ненадійний)	L2TP канал управління (надійний)
Транспортування пакетів (UDP, FR, ATM тощо)	

Рис. 2.11 Структура протоколу L2TP

Обидва L2TP і IPsec повинні підтримуватися як VPN-клієнт, так і VPN-сервером.

Для передачі повідомлень по зашифрованому каналу зв’язку протокол L2TP використовує протокол транспортного рівня UDP та два типи контрольних пакетів, що підтримують роботу віртуального тунелю. Пакети в протоколі L2TP діляться на керуючі, що впливають загалом на встановлення надійного каналу в рамках даного

протоколу та функціонал створеного тунелю, та інформаційні, впливають на процес інкапсуляції пакетів, що надходять до віртуального тунелю.

Рис. 2.12 Шифрування пакетів протоколу L2TP

На даний час протокол L2TP визнаний одним із найкраще захищених через поєднання L2TP / IPsec, але все ж таки існують негаразди:

1. Для функціонування протоколу L2TP необхідна підтримка ISP
2. Протокол L2TP має чіткі рамки у межах побудованого тунелю, що блокує свободу користувача в Internet мережі.
3. L2TP забезпечує стандартне шифрування в IP мережі за домопомогою IPsec[10].

Канальний протокол L2TP однозначно деякими критеріями схожий на протокол PPTP, через відсутність шифрування, покладаючись на протокол PPP. На жаль, протокол PPTP VPN не може надати цілісності на конфіденційності передачі пакетів на відмінну від протоколу L2TP.

Розглянемо детальніше протокол IPSec мережевого рівня моделі OSI. Для забезпечення безпечного віддаленого доступу організація може використовувати клієнтське програмне забезпечення IPSec VPN, щоб віддалені користувачі могли безпечно підключатися до внутрішніх мереж. Даний протокол розроблений для

комбінованого використання разом з протоколами IPv4 та IPv6, для забезпечення надійного криптографічного захисту інформації.

IPSec - це набір різних відкритих алгоритмів шифрування даних, що працюють поверх стека IP. Він надає служби аутентифікації і шифрування даних на мережевому рівні і може бути представлений на будь-якому пристрої, який працює по протоколу IP[8]. Щоб домогтися конфіденційності передачі використовують два головних протоколи безпеки, такі як заголовок автентифікації (AH- Authentication Header) та інкапсуляції пакетів (ESP- Encapsulating Security Payload), та протоколів обміну криптографічними ключами через мережу Internet (IKE-Internet Key Exchange), що забезпечують режим роботи в захищеному вигляді.

Рис. 2.13 Архітектура IPSec

Існує два основних режими для передачі пакетів даних між двома різними мережами, з якими працює IPsec VPN. Режим транспортування та тунелювання. Саме в першому режимі усі дані підтягаються шифруванню та передаються параметри захисту у заголовку IP-протоколу , у режимі тунелювання інкапсулюється увесь пакет даних, який і є носієм параметрів захисту. Перевагою даного протоколу над іншими заключається в тому, що можна користуватися послугами мережі з використанням комбінованого захисту можливостей інших протоколів шифрування, для забезпечення майже 100 відсоткової надійності передачі.

Популярність даний протокол отримав через свою простоту використання, адже для налаштування IPSec потрібно лише підняти політику безпеки протоколу. Даний протокол застосовується для захисту усього IP-трафіка, він також працює на канальному рівні для роботи з тунельними протоколами (L2TP / IPsec).Але слід пам’ятати, що від правильної конфігурації IPSec, залежить надійність передачі даних Протокол IPSec на даний час може гарантувати майже 100 відсоткову передачу даних, але так як він інкапсулює передані дані двічі, це суттєво зменшує його швидкодію, у порівнянні з SSL OpenVPN или SSTP.

Для підвищення захисту віртуальних приватних мереж на основі шифрування можна застосувати разом з технологіями VPN на основі розмежування трафіку. Технологія розмежування трафіку неодноразово критикувалася за ненадійність безпеки, однак на сьогодні дана проблема має способи вирішення наприклад, за допомогою мережі VPN на основі протоколів IPSec и SSL.

Широкої популярності набуває побудова VPN на основі протоколу SSL(Secure Sockets Layer) та TLS(Transport Layer Security)[10]. SSL VPN будується за допомогою криптографічних методів шифрування інформації, що надає безпечний доступ з вашого персонального ПК до різних серверів Internet-додатків. Це відбувається завдяки тому, що веб-браузери вже інтегровані під SSL, такий захист даних має не тільки надійність, а й простоту реалізації, адже не потребує постійних налаштувань від користувача.

Технологія VPN(Virtual Private Network) дозволяє створювати мережі з високим рівнем безпеки з використанням розподіленої або загальнодоступною мережевої інфраструктури VPN використовує різні правила безпеки та управління всередині мереж. Він може бути налаштований з використанням різних каналів зв'язку, таких як Інтернет або окрема інфраструктура зв'язку провайдера.

Проведемо більш детальну порівняльну характеристику найвикористаніших протоколів шифрування. Ці протоколи мають одну ціль, але різні способи побудови, методи обробки даних та їхня продуктивність над безпекою можуть відрізнятися.

PPTP (Point-to-Point Tunneling Protocol)

Даний протокол дуже швидкий у порівнянню з іншими криптографічними протоколами, що дає йому перевагу у широколосному використанні для передачі аудіо, відеофайлів. Реалізувати PPTP можна на всіх операційних системах, без додаткового обладнання. Для своєї роботи PPTP потребує найменше обчислювальних ресурсів.

Сумісність платформи	Windows, macOS, Android, iOS, Linux та ін
Шифрування VPN	До 128-розрядних.
Шифрування стандарту безпеки VPN	Відомі вразливості.
Швидкість VPN	висока швидкість через нижчий рівень шифрування)

Рис. 2.14 Характеристики протоколу PPTP

Хоча PPTP икористовує 128-бітне шифрування, але після включення даного протокола до складу Windows 95 OSR2, став набагато вразливіше через використання MS-CHAP v.2. Хоча дану проблему працівники компанії Microsoft вирішили, але за їхніми словами краще використовувати більш надійніші протоколи шифрування VPN такі як L2TP,STP.

Отже, для всіх намірів і цілей PPTP застаріла як технологія конфіденційності та безпеки. Якщо це те, що шукає організація, тоді організації слід вибрати інший протокол.

Якщо організація хочете розблокувати лише заблоковані веб-сайти, можливо, варто звернути увагу на постачальника VPN, який пропонує PPTP. Однак у такому випадку може бути кращою ідеєю використовувати іншу технологію, таку як Smart DNS або Proxy, яка не претендує на забезпечення конфіденційності та безпеки, але надасть георозблокування.

L2TP/IPsec (Layer 2 Tunneling Protocol)

Найбільш поширене сполучення з L2TP - це набір протоколів безпеки, відомий як IPsec або просто безпека Інтернет-протоколу.

Сумісність із платформою	Windows, macOS, Android, iOS, Linux та ін.
Шифрування VPN	До 256-бітного.
Сильне шифрування VPN Security	Сильна цілісність даних.
Швидкість VPN	Відносно повільна завдяки обробці даних процесором.

Рис. 2.15 Характеристики протоколу L2TP/IPsec

Це IPsec, який фактично містить технологію, яка обробляє аутентифікацію між комп'ютером та сервером VPN[11]. IPsec також містить технологію шифрування пакетів даних із сильним рівнем шифрування. Це робить майже неможливим отримати зашифровані дані.

SSTP (Secure Socket Tunneling Protocol)

SSTP - протокол безпечного тунелювання сокетів, був створений компанією Microsoft для роботи з Windows Vista, але на сьогоднішній день має підтримку таких платформа як SEIL, Linux, RouterOS.

Сумісність із платформою	Windows, macOS, Android, Linux та ін.
Шифрування VPN	До 256-бітного.
Сильне шифрування VPN Security	Шифрування SSL включено
Шифрування SSL включено	Повільна швидкість (завдяки високому рівню безпеки).

Рис. 2.16 Характеристики протоколу SSTP

Перевагою є те, що він інтегрований саме з Windows, що надає шанс отримати доступ до SSTP як спосіб подолати блокування VPN, та можливості обходити брандмауєри NAT[11].

SSL використовується в даному випадку для забезпечення узгодження ключа, шифрування і захисту цілісності.

OpenVPN

OpenVPN - це програмний продукт з відкритим вихідним кодом, розпод остраняет під ліцензією GNU General Public License (GPL), який може використовуватися для встановлення VPN-звязку між двома компютерами в локальній бізнес-мережі через інфраструктуру загальнодоступною звязку. Він використовує спеціальні протоколи безпеки і 256-бітове шифрування і здатний обходити транслятори мережевих адрес (NAT) і брандмауери[12].

Сумісність із платформою	Windows, macOS, Android, iOS, Linux, маршрутизатори тощо.
Шифрування VPN	До 256-бітного.
VPN безпека	Найвища безпека; Цифрова сертифікація.
VPN швидкість	швидкий, незважаючи на високий рівень безпеки

Рис. 2.17 Характеристики протоколу OpenVPN

Це дозволяє комп’ютерам аутентифікувати один одного з використанням загального секретного ключа, сертифікатів або імені користувача та пароля. Це протокол, який справді повністю може задовольнити кіберпростір, надавши найбільшу безпеку при передачі даних, адже OpenVPN використовує OpenSSL та TLS в основному. Так як даний протокол, на відміну від PPTP, SSTP, не має вбудованої підтримки для операційної системи[14].

Оскільки OpenVPN 2.0, спеціальний серверний режим дозволяє з'єднувати декілька вхідних портів TCP або UDP одного і того ж, використовуючи іншу конфігурацію для кожного окремого з'єднання, наприклад, порт TCP 443. OpenVPN може працювати на сайтах, які використовують протокол HTTPS, ухилятися від блокування VPN на основі порта. Підключення OpenVPN можна тунелювати майже через кожен тунель брандмауера. OpenVPN використовує бібліотеку OpenSSL, вона має доступ до всіх технологій шифрування,наприклад 3DES, AES, Camellia, Blowfish, CAST-128, що входять до цієї бібліотеки. Однак рідко застосовується

будь-яке, крім шифрування Blowfish та AES, що добре, якщо достатня довжина ключа. AES, за словами фахівців, технологія, що немає вразливостей і використовується державними установами і секретними службами. Швидкодія даного протоколу залежить від рівня шифрування і у деяких моментах вона швидше ніж IPSec, але встановлення і конфігурування даного протоколу набагато складніше ніж L2TP/IPSec и PPTP.

Перевагою VPN, що використовує Openvpn, є те, що місцева мережа буде широкою, час, який потрібен для підключення локальної мережі до інших місць також стає швидше. Скорочення оперативних витрат в порівнянні з використанням орендованої лінії в якості традиційного способу впровадження PBC. VPN може знизити вартість створення мережі, тому що вона не вимагає проводів (орендована лінія). Збільшити масштабованість, а також полегшити доступ з будь-якого місця, тому що VPN для підключення до Інтернету (віддалений доступ). Openvpn використовує механізм Secure Sockets Layer / Transport Layer Security (SSL / TLS), SSL / TLS використовує один з кращих методів шифрування, а саме асиметричне шифрування. На асиметричному шифруванні кожен сервер і клієнт має два ключа, а саме відкритий ключ і закритий ключ.

За даними наукового журналу «Технічні науки та технології» протокол OpenVPN визнали найбезпечнішим протоколом для шифрування даних.

IKEV2/IPsec

Перша версія протоколу була випущена ще у 1998 році як колекція з трьох IETF Rfc (2407, 2408 і 2409)[20]. Через обмеження і складності IKEv1, IETF вирішив запропонувати другий варіант IKEv2 що є злиттям різних протоколів з технологіями безпеки IPsec. Internet Key Exchange (IKE) був першим в світі AKE, в якому використовувалися методи збереження конфіденційності. IKEv2 був організований для мобільних технологій, що підтримують технологію "мультихомінг", дозволяючи переходити з Wi-Fi мережі до мобільного підключення Інтернету, не випадаючи з тунелю VPN[26]. Даний протокол за такими обставинами модна вважати найшвидшим протоколом, але з боку клієнтоорінтовності він часто IKEv2 піддається атакам типу «відмова в обслуговуванні» (DoS), заснованим на

фрагментах IP і атаках з використанням вироджених повідомлень, мала кількість підтримуючих платформ, порт UDP 500 блокується простіше, ніж рішення на основі SSL, як, наприклад, SSTP або OpenVPN, налаштування на сервер досить важка, це може викликати потенційні проблем з боку безпеки.

Висновки:

Технологія VPN дозволяє ефективно вирішувати завдання щодо забезпечення безпеки інформаційних ресурсів, підтримати цілісність та конфіденційність інформації, що передається в локальних і глобальних інформаційних середовищах.

Технологія VPN забезпечує зв'язок між мережами, а також між віддаленим користувачем і корпоративними мережами за допомогою захищеного каналу (тунелю), «прокладеного» в загальнодоступній мережі Internet.

Відповідно, захист конфіденційності інформації від небажаного втручання дуже відповідальна та актуальна задача на сьогоднішній день, адже, повністю захистити інформацію неможливо, тому технології захисту даних ґрунтуються на застосуванні сучасних методів, які запобігають перехоплення інформації та її втрати. На сьогоднішній день найкращим способом зберегти цілісність даних є криптографічні методи захисту інформації із використанням шифрування.

	Шифрування	**Безпеки**	**Швидкість**
OpenVPN	256-біт	Найвище шифрування	Швидкий на високих латентних з'єднання
L2TP	256-біт	Найвище шифрування	Повільний і сильно процесорний
SSTP	256-біт	Найвище шифрування	Сповільнений
IKEv2	256-біт	Найвище шифрування	Швидкий
PPTP	128-біт	Мінімальна безпека	Швидкий

Рис. 2.18 Основні характеристики протоколів шифрування

В залежності від цілей зберігання інформації та від її виду використання протоколів шифрування можна поділити на декілька категорій. Одні доцільно

використовувати для максимального захисту, нехтуючи швидкістю та продуктивністю, інші, навпаки, через свою продуктивність та пропускну здатність стають повільними та сильнопроцесорними, що сповільнює роботу передачі даних[24].

Отже, з проведеного аналізу, що був представлений в другому розділі, можна підсумувати і зробити висновки, що на даний час OpenVPN своїми характеристиками може задовольнити поставлені задачі, адже конфігурування, рівень безпеки, підтримка різних складних алгоритмів надають системі надійного захисту.

РОЗДІЛ 3.
ПРАКТИЧНЕ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ OPENVPN

3.1 Алгоритм налаштування параметрів OpenVPN

Етапи налаштування і встановлення з'єднання OpenVPN:

1. Встановлення OpenVPN
2. Створення директорії центру сертифікації
3. Налаштування змінних центру сертифікації
4. Створення центру сертифікації
5. Створення сертифіката, ключа і файлів шифрування для сервера
6. Створення сертифіката і пари ключів для клієнта
7. Налаштування сервісу OpenVPN
8. Налаштування мережевої конфігурації сервера
9. Включення сервісу OpenVPN
10. Створення конфігурацій клієнтів
11. Встановлення з'єднання

Перш за все необхідно налаштувати сервер з Ubuntu та окремий, чи не-рутовий (non-root) профіль користувача з привілеями sudo на сервері. Також необхідно налаштувати фаєрвол. В Ubuntu налаштування OpenVPN відбувається в наступним чином:

1. Встановлення OpenVPN

Оновимо список пакетів сервера і встановимо необхідні пакети наступними командами:

```
sudo apt-get update
sudo apt-get install openvpn easy-rsa
```

Необхідне програмне забезпечення встановлено і готове до налаштування.

2. Створення директорії центру сертифікації

OpenVPN це віртуальна приватна мережа, що використовує TLS / SSL. Це означає, що OpenVPN використовує сертифікати для шифрування трафіку між

сервером і клієнтами. Для випуску довірених сертифікатів (trusted certificates) потрібно створити власний центр сертифікації.

Для початку скопіюємо шаблонну директорію easy-rsa в нашу домашню директорію за допомогою команди make-cadir:

make-cadir ~/openvpn-ca

Далі зайдемо в цю директорію для початку налаштування ЦС:

cd ~/openvpn-ca

3. Налаштування змінних центру сертифікації

Для налаштування змінних центру сертифікації необхідно відредагувати файл vars. Відкрийте цей файл у текстовому редакторі:

nano vars

Всередині файлу ви знайдете змінні, які можна відредагувати, і які задають параметри сертифікатів при їх створенні. Нам потрібно змінити лише кілька змінних

export KEY_COUNTRY="US"

export KEY_PROVINCE="NY"

export KEY_CITY="New York City"

export KEY_ORG="DigitalOcean"

export KEY_EMAIL="admin@example.com"

export KEY_OU="Community"

export KEY_NAME="server"

4. Створення центру сертифікації

Переконайтеся, що ви перебуваєте в директорії центру сертифікації і використовуйте команду sourceдо файлу vars:

cd ~/openvpn-ca

source vars

Ви повинні побачити наступний висновок:

NOTE: If you run ./clean-all, I will be doing a rm -rf on /home/sammy/openvpn-ca/keys

Ця команда запустить процес створення ключа і сертифіката кореневого центру сертифікації. Оскільки ми задали всі змінні у файлі vars, всі необхідні

значення будуть введені автоматично. Тепер у нас є центр сертифікації, який ми зможемо використовувати для створення всіх інших необхідних нам файлів.

5. Створення сертифіката, ключа і файлів шифрування для сервера

Далі створимо сертифікат, пару ключів і деякі додаткові файли, які використовуються для здійснення шифрування, для нашого сервера.

Почнемо зі створення сертифіката OpenVPN і ключів для сервера. Це можна зробити за допомогою такої команди:

./build-key-server server

Погодьтеся з усіма значеннями за замовчуванням, натискаючи ENTER . Не ставте challenge password. В кінці процесу два рази введіть у для підпису і підтвердження створення сертифіката:

Certificate is to be certified until May 1 17:51:16 2026 GMT (3650 days)

Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y

Write out database with 1 new entries

Data Base Updated

Далі створимо залишилися файли. Ми можемо згенерувати сильні ключі протоколу Діффі-Хеллмана, використовувані при обміні ключами, командою:

./build-dh

Для завершення цієї команди може знадобитися кілька хвилин.

Далі ми можемо згенерувати підпис HMAC для посилення здатності сервера перевіряти цілісність TSL:

openvpn --genkey --secret keys/ta.key

6. Створення сертифіката і пари ключів для клієнта

Далі ми можемо згенерувати сертифікат і пару ключів для клієнта. Взагалі це можна зробити і на клієнтській машині і потім підписати отриманий ключ центром сертифікації сервера, для простоти ми згенерируем підписаний ключ на сервері.

cd ~/openvpn-ca

source vars

./build-key client1

В ході процесу створення файлів все значення за замовчуванням будуть введені, ви можете натискати ENTER.

7. Налаштування сервісу OpenVPN

Спочатку скопіюємо створені нами файли. Вони знаходяться в директорії ~/openvpn-ca/keys, в якій вони і були створені. Нам потрібно створити сертифікат і ключ центру сертифікації, сертифікат і ключ сервера, підпис HMAC і файл Diffie-Hellman:

cd ~/openvpn-ca/keys

sudo cp ca.crt ca.key server.crt server.key ta.key dh2048.pem /etc/openvpn

Далі нам необхідно скопіювати і розпакувати файл-приклад конфігурації OpenVPN в конфігураційну директорію, ми будемо використовувати цей файл в якості бази для наших налаштувань:

gunzip -c /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz | sudo tee /etc/openvpn/server.conf

Налаштування конфігурації OpenVPN

Тепер, коли наші файли знаходяться на своєму місці, займемося налаштуванням конфігураційного файлу сервера:

sudo nano /etc/openvpn/server.conf

Базова настройка

Спочатку знайдемо секцію HMAC пошуком директиви tls-auth. Видаліть ";" для того, щоб розкоментувати рядок з tls-auth. Далі додайте параметр key-directioni встановіть його значення в "0":

tls-auth ta.key 0 # This file is secret

key-direction 0

Далі знайдемо секцію шифрування, нас цікавлять закоментовані рядки cipher. Шифр AES-128-CBCзабезпечує хороший рівень шифрування і широко підтримується іншими програмними продуктами. Видаліть ";" для раскомментірованія рядки AES-128-CBC:

cipher AES-128-CBC

Під цим рядком додайте рядок authi виберіть алгоритм HMAC. Хорошим вибором буде SHA256:

auth SHA256

8. Налаштування мережевої конфігурації сервера

Далі нам необхідно налаштувати мережеву конфігурацію сервера, щоб OpenVPN міг коректно перенаправляти трафік.

Налаштування перенаправлення IP

Спочатку вирішимо сервера перенаправляти трафік. Це ключова функціональність нашого VPN сервера.

Налаштуємо це в файлі /etc/sysctl.conf:

sudo nano /etc/sysctl.conf

Знайдіть рядок настройки net.ipv4.ip_forward. Видаліть "#" з початку рядка, щоб розкоментувати її:

net.ipv4.ip_forward=1

Для застосування налаштувань до поточної сесії наберіть команду:

sudo sysctl -p

Налаштування правил UFW для приховування з'єднань клієнтів

Перед тим, як змінити цей файл, ми повинні знайти публічний інтерфейс мережі (public network interface). Для цього наберіть команду:

ip route | grep default

Публічний інтерфейс повинен слідувати за словом "dev". Наприклад, в нашому випадку цей інтерфейс називається enp0s3:

192.168.56.0/24 dev enp0s3 proto kernel scope link src 192.168.56.1

Знаючи назву інтерфейсу відкриємо файл /etc/ufw/before.rulesi додамо туди відповідні налаштування:

sudo nano /etc/ufw/before.rules

Це файл містить настройки UFW, яке застосовуються перед застосуванням правил UFW. Додайте в початок файлу виділені червоним рядки. Це налаштує правила, які застосовуються по замовчуванню, до ланцюжка POSTROUTINGв таблиці nati буде приховувати весь трафік від VPN:

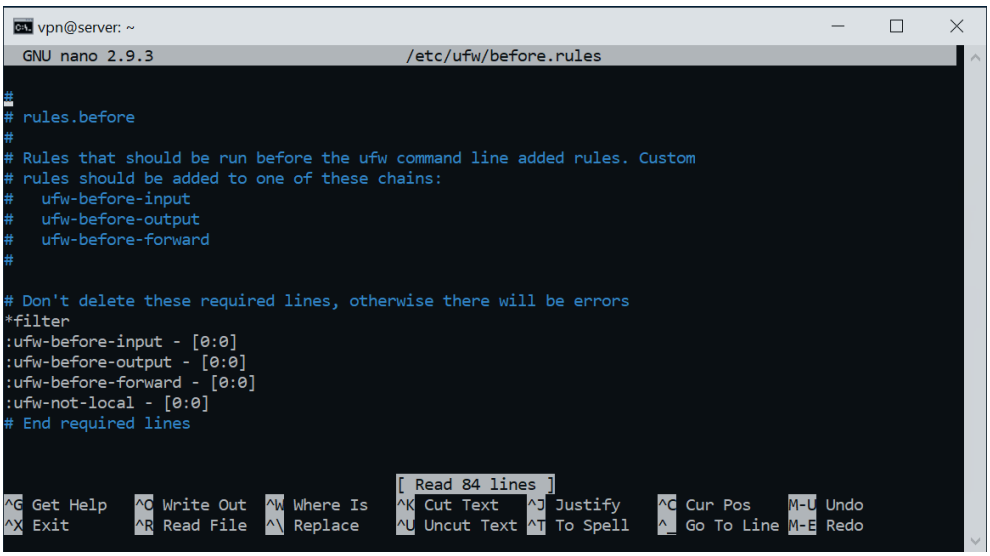

Рис. 3.1 Налаштування правил

Тепер ми повинні повідомити UFW, що йому за замовчуванням необхідно вирішувати переслані пакети. Для цього відкрийте файл /etc/default/ufw:

sudo nano /etc/default/ufw

Знайдіть у файлі директиву DEFAULT_FORWARD_POLICY. Ми змінимо значення з DROPна ACCEPT:

DEFAULT_FORWARD_POLICY="ACCEPT"

Відкриття порту OpenVPN і застосування зміни

sudo ufw allow 1194/udp

sudo ufw allow OpenSSH

Тепер деактивувавши і активуємо UFW для застосування внесених змін:

sudo ufw disable

sudo ufw enable

Тепер наш сервер налаштований для обробки трафіку OpenVPN.

9. Включення сервісу OpenVPN

Ми готові включить сервіс OpenVPN на нашому сервері. Ми можемо зробити це за допомогою systemd. Необхідно запустити сервер OpenVPN вказавши ім'я нашого файлу конфігурації в якості змінної після імені файлу systemd. Файл конфігурації для нашого сервера називається , тому ми додамо в кінець імені файлу при його виклику:/etc/openvpn/server.conf@server

sudo systemctl start openvpn@server

Переконаємося, що сервіс успішно запущений командою:

sudo systemctl status openvpn@server

Якщо все вийшло, висновок повинен виглядати приблизно так:

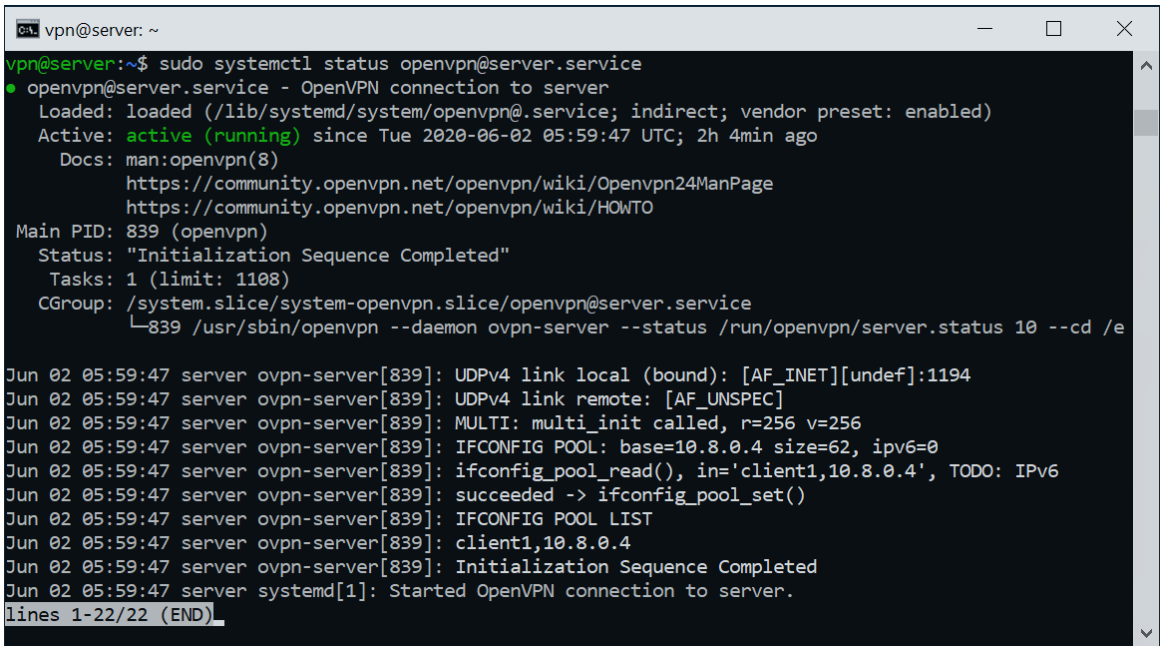

Рис. 3.2 Перевірка піднятого сервісу

Також можна перевірити доступність інтерфейсу OpenVPN tun0 наступною командою:

ip addr show tun0

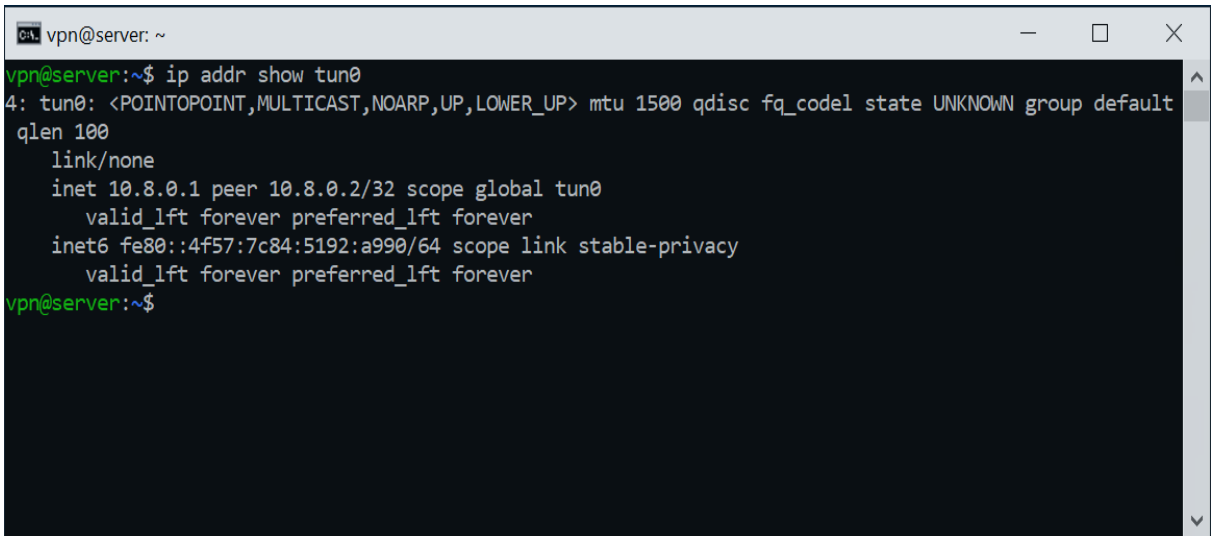

Рис. 3.3 Перевірка піднятого інтерфейсу OpenVPN

Налаштуємо сервіс на автоматичне включення при завантаженні сервера:

sudo systemctl enable openvpn@server

10. Створення конфігурації клієнтів

Використаємо приклад із базової конфігурації та додамо в нього сертифікати CA, серверу та клієнта для зручності.

```
client
dev tun
proto udp
remote 192.168.56.1 1194
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
cipher BF-CBC
auth SHA256
key-direction 1
verb 3
```

Рис. 3.4 Конфігурація клієнта

11. Встановлення файлу конфігурації клієнта у Windows10

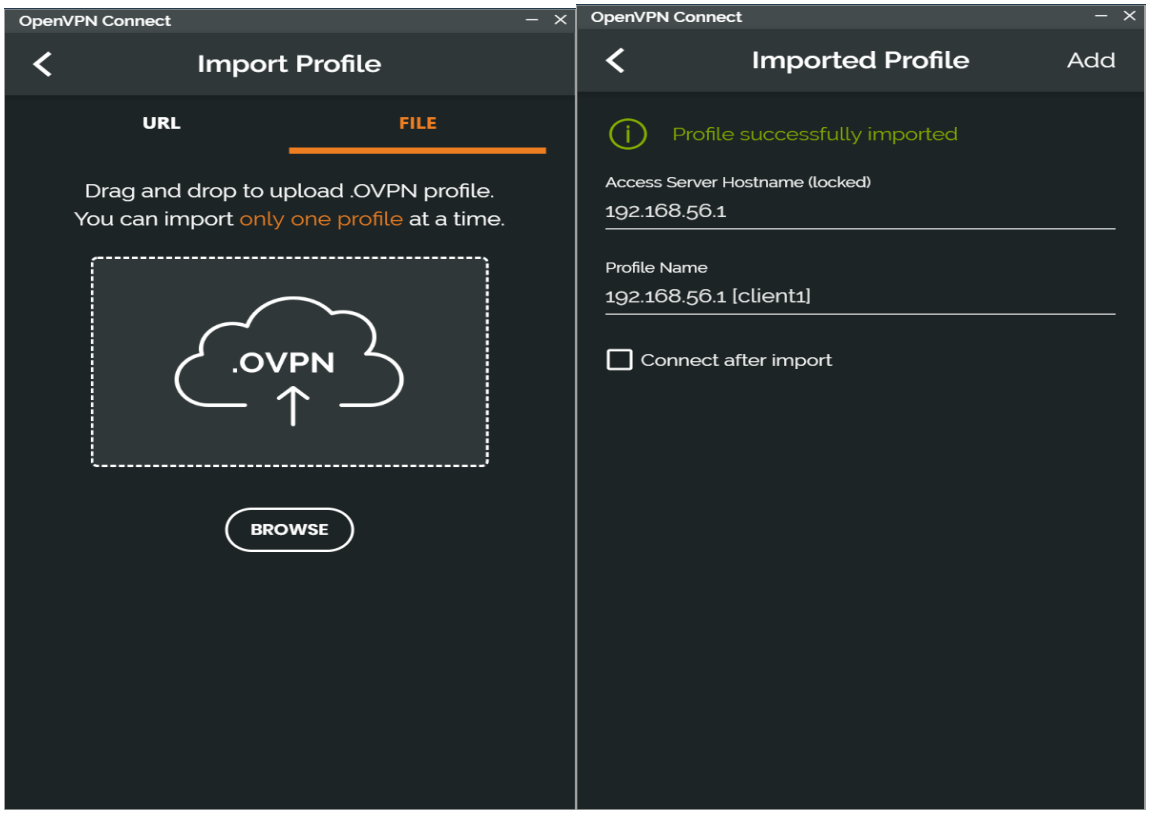

Рис. 3.5 Встановлення конфігурації клієнта

12. Встановлення з’єднання клієнта з VPN сервером

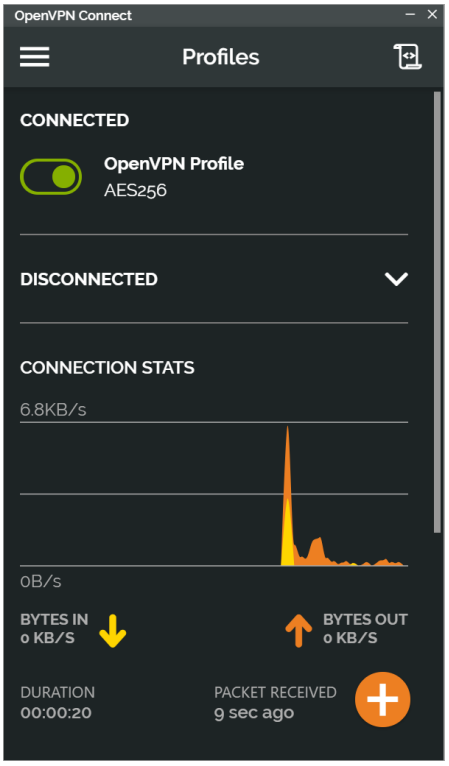

Рис. 3.6 Підключення з VPN сервером

3.2 Аналіз впливу шифрування на канал зв’язку у технології OpenVPN

Для того, щоб проаналізувати впливу шифрування на канал зв’язку можна використовувати пропускну здатність, так як застосування технології OpenVPN з різними видами шифрування найбільше впливають на неї.

- Аналіз проводився у віртуальному середовищі VirtualBox.

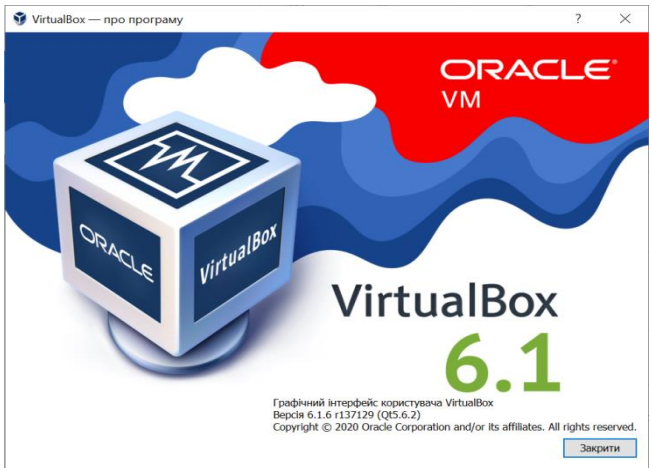

Рис. 3.7 Середовище VirtualBox

У віртуальному середовищі VirtualBox було створену мережу 192.168.56.0/24 між віртуальною машиною з операційною системою Ubuntu, яка виступає в ролі VPN сервера та хост-машиною, яка виспуає в ролі клієнта. В якості генератора трафіка та інструмента вимірювання використано Iperf версії 3.1.3, який був встановлений на двох кінцевих точках з операційною системою Ubuntu та Windows 10 – один діє як клієнт, тобто передавач трафіку, а другий як сервер, тобто приймач трафіку.

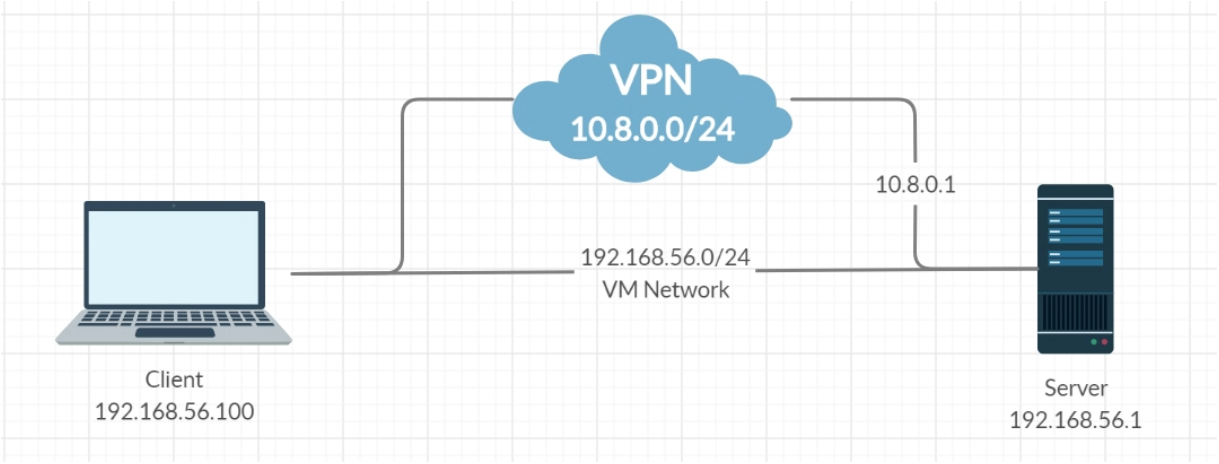

Рис. 3.8 Схема підключення обладнання у VirtualBox

1. Тест каналу зв’язку VM Network без VPN тунелю

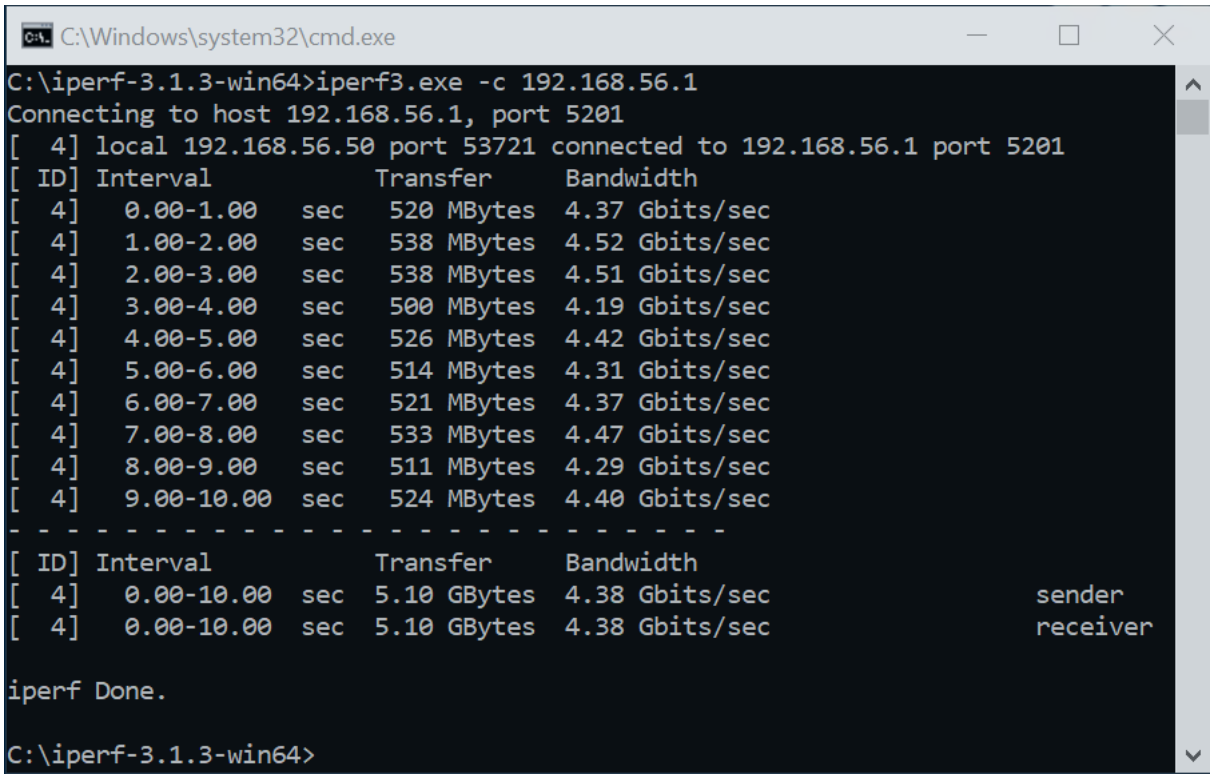

Рис. 3.9 Пропускна здатність VM Network

2. Тест каналу зв’язку VPN тунелю без шифрування

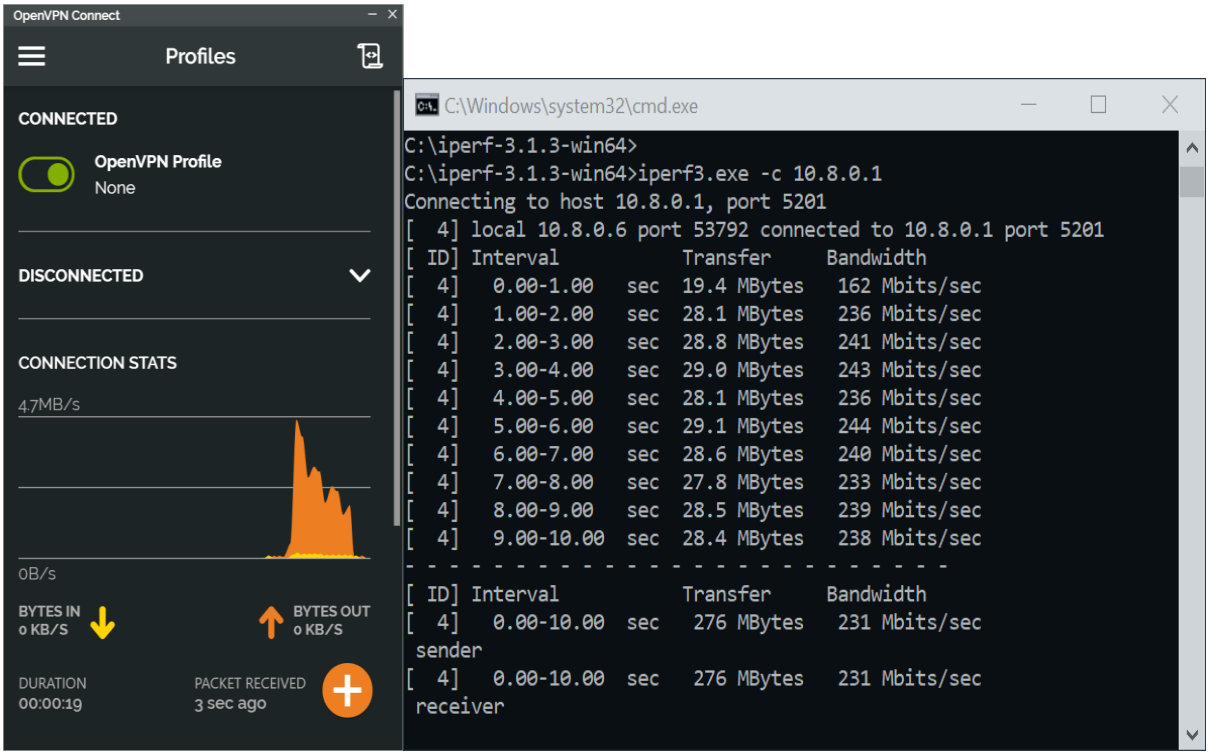

Рис. 3.8 Пропускна здатність VPN без шифрування

3. Тест каналу зв’язку VPN тунелю з шифруванням DES-EDE

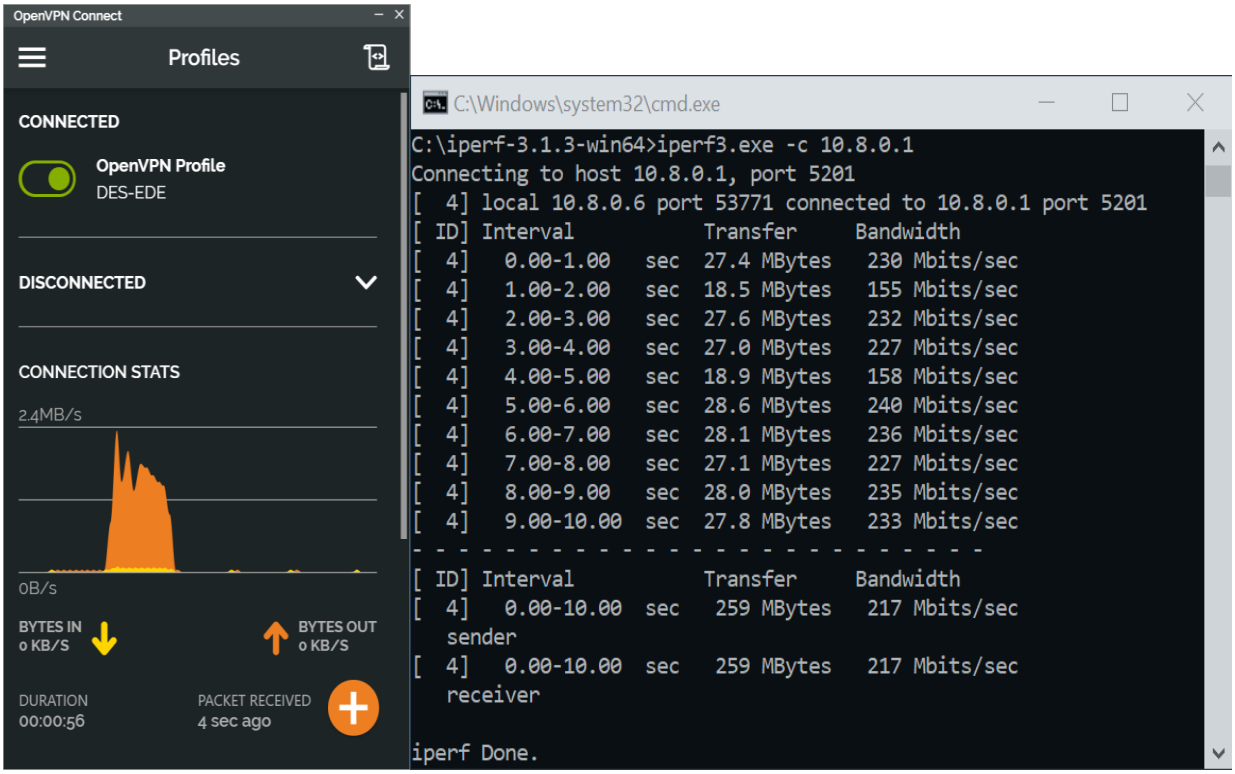

Рис. 3.9 Пропускна здатність VPN з DES-EDE

4. Тест каналу зв’язку VPN тунелю з шифруванням BF-CBC

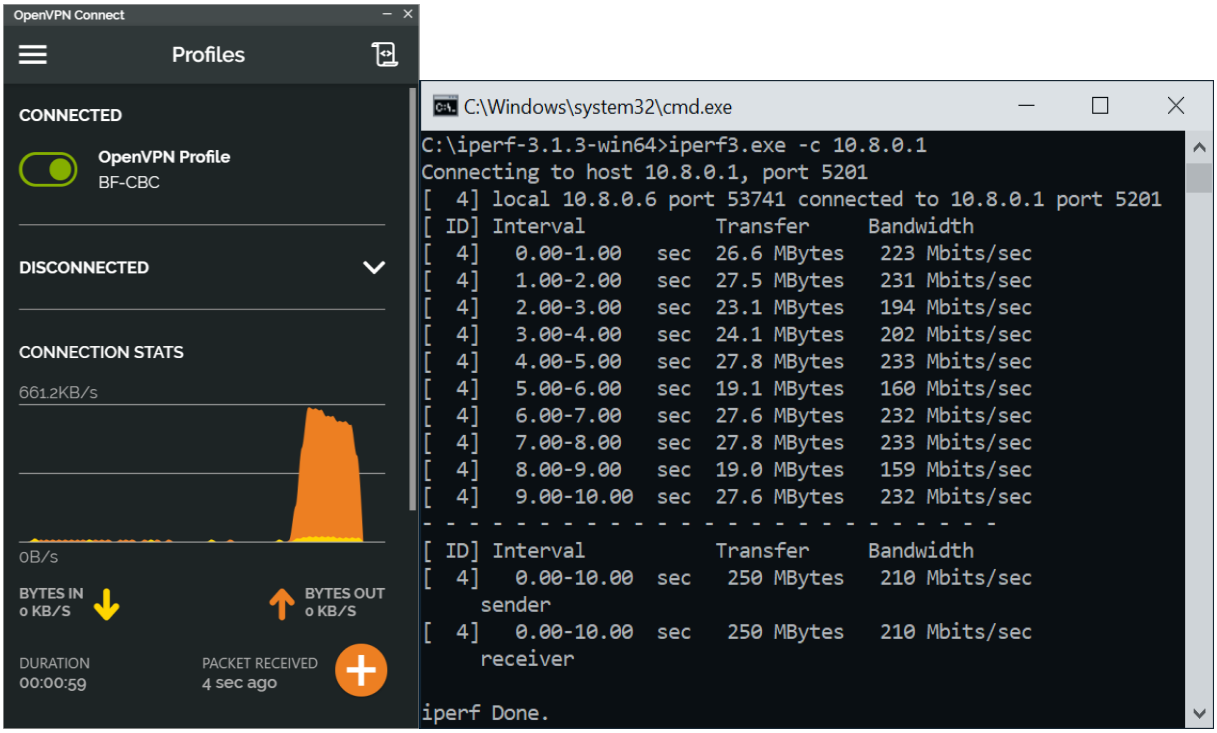

Рис. 3.10 Пропускна здатність VPN з BF-CBC

5. Тест каналу зв’язку VPN тунелю з шифруванням AES-256

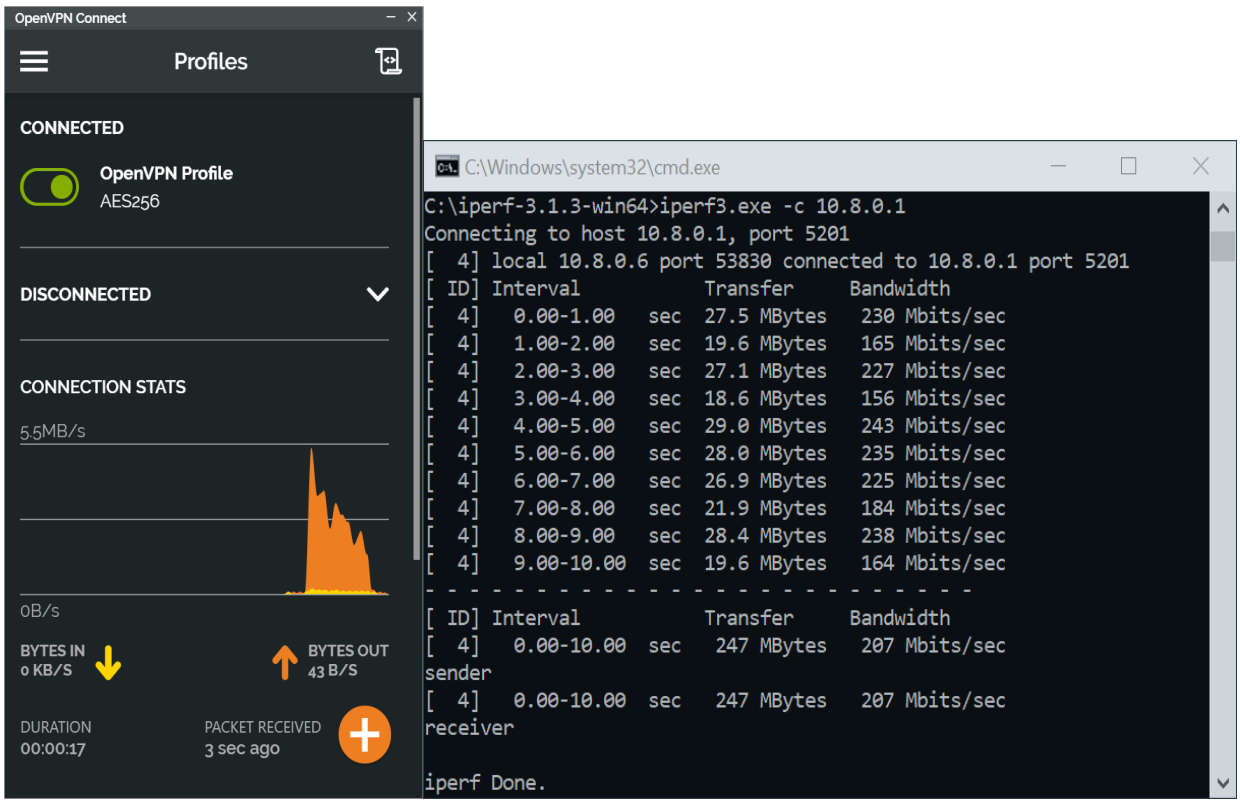

Рис. 3.11 Пропускна здатність VPN з AES-256

Висновки:

В ході аналізу залежності пропускної здатності OpenVPN від параметрів шифрування, було описано та проведено налаштування OpenVPN серверу на базі операційної системи Ubuntu, а також процес створення конфігурації для клієнта.

Результати аналізу показують, що вплив шифрування на канал зв’язку OpenVPN є незначним, але пропускна здатність самого каналу VPN, навіть без шифрування, значно менша ніж доступна пропускна здатність VM Network. Таким чином, OpenVPN може бути рекомендований для застосування у мережах зв’язку, для захисту конфіденційної інформації, із застосуванням найбільш стійких алгоритмів шифрування.

ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ

В дипломній роботі проаналізовано основні види інформації, що потребує захист при передачі по каналам зв'язку. Досліджено основні аспекти побудови віртуальних приватних захищених мереж для передачі цілісності інформації по лініям зв'язку, адже захист конфіденційності інформації від небажаного втручання дуже відповідальна та актуальна проблема на сьогоднішній день, що залучає усі державні сфери для вирішення даної задачі. Проаналізовано класифікацію віртуальних приватних мереж та їхнє призначення, принципи їх побудови, необхідні умови для повноцінного функціонування. Досліджено основні методи захисту інформації від несанкціонованого доступу, що можуть бути реалізовані впливом природного або штучного характеру у VPN мережах.

Завданням захисту інформації полягає у тому, щоб шахраї якомога довше не змогли завдати шкоди системі зв'язку, саме для цього потрібні все більше новітніх методів і алгоритмів збереження даних.

Саме тому велику увагу приділяється аналізу основних криптографічних методів і способів захисту інформації на основі VPN-мережі. Наведено переваги та недоліки, які притаманні протоколам шифрування. Проведений порівняльний аналіз ефективності застосування, переваги і недоліки методів криптографічного захисту інформації на основі VPN.

Досліджено вплив шифрування на канал зв'язку OpenVPN, проаналізовано пропускну здатність та ефективність використання складних криптографічних методів. Для досягнення поставленої мети було проведено практичне виконання залежності пропускної здатності OpenVPN від параметрів шифрування, було описано та проведено налаштування OpenVPN серверу на базі операційної системи Ubuntu, а також процес створення конфігурації для клієнта.

Отримані результати дозволяють ефективно обирати відповідно до типу інформації та способу її передачі шифри, що максимально задовільнять високий рівень захисту, та більшу продуктивність.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закони України: «Про електронні документи і електронний документообіг»// електрон.текст. дані URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення 16.05.2020)
2. Закони України: «Про інформацію»// електрон.текст. дані URL: https://zakon.rada.gov.ua/laws/show/12657-12 (дата звернення 16.05.2020)
3. Experimental estimation of channel width of IP BPX subscribers in OpenVPN IP networks// електрон. текст. дані URL: https://medium.com/datadriveninvestor/4-stages-of-iot-architecture-explained-in-simple-words-b2ea8b4f777f(дата звернення: 04.05.2020)
4. Experimental performance comparison between TCP vs UDP tunnel using OpenVPN//електрон.текст. дані URL: https://medium.com/datadriveninvestor/4-stages-of-iot-architecture-explained-in-simple-words-b2ea8b4f777f(дата звернення: 04.05.2020)
5. Биячуев Т. БЕЗПЕКА КОРПОРАТИВНИХ МЕРЕЖ / Т.А. Биячуев. – СПб: СПб ДУ ІТМО, 2004. – 161 с.(дата звернення: 04.05.2020)
6. Основи захисту інформації в телекомунікаційних та комп’ютерних мережах / Л.Гончарова, А. Возненко, О. Стасюк, Ю. Коваль. – К., 2013. – 435 с. (дата звернення: 08.05.2020)
7. Исагулиев Карэн Паруйрович. Справочник по криптологии . - Минск : ООО "Новое знание", 2004. - 236с. (дата звернення: 08.05.2020)
8. Лук'янов Дмитро Олександрович. Управління ключовою інформацією в системах захисту групових комунікацій : Автореф. дис... канд. фіз.-мат. наук: 01.05.03 / Київський національний ун-т ім. Т.Г.Шевченка - К., 2004. - 16с. (дата звернення: 08.05.2020)
9. IP-СПУФИНГ. МЕТОДЫ ОПРЕДЕЛЕНИЯ И ОСЛАБЛЕНИЯ АТАКИ// електрон.текст. дані URL: https://medium.com/datadriveninvestor/4-stages-of-iot-architecture-explained-in-simple-words-b2ea8b4f777f (дата звернення: 08.05.2020)
10. Canavan J. Fundamentals of Network Security / John E. Canavan. – Boston • London: Artech House, 2001. – 218 с. 5-18(дата звернення 10.05.2020)

11. Attack a network by using a rogue DHCP server// електрон.текст. дані URL: https://medium.com/datadriveninvestor/4-stages-of-iot-architecture-explained-in-simple-words-b2ea8b4f777f (дата звернення: 10.05.2020)

12. Гроздов Глеб Геннадьевич. Современные методы криптографической защиты информации: (обзор по материалам открытой печати) . - К., 2002. - 31с. : рис. - (Препр. / 2002; 01). - Библиогр.: с. 28-30(дата звернення: 10.05.2020).

13. Безпека інформаційних систем// електрон.текст. дані URL: http://pidruchniki.com/74227/informatika/bezpeka_informatsiynih_sistem(дата звернення 15.05.2020)

14. Богуш В. М., Довидьков О. А., Кудін А.М. / Перспективи розвитку автоматизованих систем обробки конфіденційної інформації загального призначення / Вісник Державного університету інформаційно-комунікаційних технологій. - 2003. -Том. 1. - №1.(дата звернення 18.05.2020)

15. Шаньгин В.Ф. / Защита информации в компьютерных системах и сетях, 2012. – 89 с.(дата звернення 19.05.2020)

16. Ларін М.В. / Управління документацією і нові інформаційні технології. М: Наукова книга, 2001. 137 с.(дата звернення 25.05.2020)

17. Боровиков А.М., Тимошенко А.А. / Системы защиты информационного обмена «Клиент – банк» / Безопасность информации, 1995.(дата звернення 03.06.2020)

18. Гайкович В., Першин А. / Безопасность електронных банковских систем. – Единая Европа. -1994.(дата звернення 25.05.2020)

19. Бабаш Александр Владимирович, Шанкин Генрих Петрович. Криптография / В.П. Шерстюк (ред.), Э.А. Применко (ред.). - М. : ООО Издательство "Солон-Р", 2002. - 511с./ (дата звернення 25.05.2020)

20. Бардіс Ніколас. Розробка підходу і застосування апарату булевих функцій для аналізу і синтезу ефективних криптографічних алгоритмів захисту інформації : Автореф. дис... канд. техн. наук: 05.13.13 / Національний технічний ун-т України "Київський політехнічний ін-т". - К., 1998. - 16с(дата звернення 25.05.2020)

21. Горбенко Іван Дмитрович, Гріненко Тетяна Олексіївна. Захист інформації в інформаційно-телекомунікаційних системах/ Харківський національний ун-т радіоелектроніки. - Х. : ХНУРЕ, 2004. - Бібліогр.: с. 364-368(дата звернення 26.05.2020)

22. Experimental performance comparison between TCP vs UDP//електрон.текст. дані URL: https://medium.com/datadriveninvestor/4-stages-of-iot-architecture-explained-in-simple-words-b2ea8b4f777f(дата звернення: 26.05.2020)

23. Спуф атаки - Защита от DDoS атак //електрон.текст. дані URL: ресурсу: https://stopddos.pro/index.php/2018/03/14/ip-spoofing/ (дата звернення: 28.05.2020).

24. Захист інформації. Криптографічні методи : Підруч. для вищ. навч. закл. / І.І. Маракова, А.І. Рибак, Ю.С. Ямпольський; Одес. держ. Політехн. ун-т, Ін-т радіоелектрон. і телекомунікацій. - О., 2001. - 174 с. (дата звернення: 26.05.2020)

25. Форум IT фахівців //електрон.текст. дані URL: http://jak.bono.odessa.ua/articles/forum-it-fahivciv.php(дата звернення: 26.05.2020)

26. Мельников Виталий Викторович. Защита информации в компьютерных системах. - М. : Финансы и статистика, 1997. - 368с. дата звернення: (28.05.2020)